ECONSTOR
Make Your Publications Visible.

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Erserbetci, Murad

Research Report

Einführung der EU-Datenschutz-Grundverordnung: Auswirkungen und Handlungsempfehlungen für die Unternehmensbereiche, Geschäftsleitung, Personal sowie Informationstechnologie

EIKV-Schriftenreihe zum Wissens- und Wertemanagement, No. 43

Provided in Cooperation with:
European Institute for Knowledge & Value Management (EIKV), Hostert (Luxembourg)

Suggested Citation: Erserbetci, Murad (2020) : Einführung der EU-Datenschutz-Grundverordnung: Auswirkungen und Handlungsempfehlungen für die Unternehmensbereiche, Geschäftsleitung, Personal sowie Informationstechnologie, EIKV-Schriftenreihe zum Wissens- und Wertemanagement, No. 43, European Institute for Knowledge & Value Management (EIKV), Hostert

This Version is available at:
https://hdl.handle.net/10419/226694

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

EIKV European Institute for Knowledge- and Value-Management A.s.b.l.

EIKV-Schriftenreihe zum
Wissens- und Wertemanagement

Einführung der EU-Datenschutz-Grundverordnung: Auswirkungen und Handlungsempfehlungen für die Unternehmensbereiche, Geschäftsleitung, Personal sowie Informationstechnologie

Murad Erserbetci

Band 43

IMPRESSUM
EIKV-Schriftenreihe zum Wissens- und Wertemanagement
Herausgeber: André Reuter, Thomas Gergen

© EIKV Luxembourg, 2016 - 2020

European Institute for Knowledge & Value Management (EIKV)
c/o M. André REUTER – 8, rue de la Source
L-6998 Hostert - GD de Luxembourg
info@eikv.org
www.eikv.org

Einführung der EU-Datenschutz-Grundverordnung: Auswirkungen und Handlungsempfehlungen für die Unternehmensbereiche, Geschäftsleitung, Personal sowie Informationstechnologie

Murad Erserbetci

Die vorliegende Arbeit wurde als Thesis zur Erlangung eines Doctorate in Business Administration (DBA) beim Business Science Institute, BSI, sowie bei der Université Jean Moulin Lyon 3 eingereicht und am 30. September in Wiltz/Luxemburg verteidigt. Betreuer der Thesis war Prof. Dr. Dr. Thomas Gergen, Maître en droit (Luxemburg).

I. Vorwort

Gewidmet meiner Frau und meinem Sohn

“Dans la vie, il n’y a pas de solutions.

Il n’y a que des forces en marche:

Il faut les créer et les solutions suivent.”

(Im Leben gibt es keine Lösungen.

Es gibt nur Kräfte, die in Bewegung sind:

Man muss sie erzeugen – und die Lösungen werden folgen).

Antoine de Saint Exupéry:

II. Inhaltsverzeichnis

Teil. 2 - Umsetzung

Teil. 3 - Handlungsempfehlungen

III. Abstract „Deutsch“

Die nachfolgende Arbeit beschreibt in drei Teilen die Einführung der **D**aten**s**chutz-**G**rund**ver**o**r**dnung (**DS-GVO**). Dabei wird eine Variante zur Umsetzung der Vorgaben der am 25.05.2018 eingeführten Datenschutz-Grundverordnung ebenfalls aufgezeigt. Im ersten Teil werden die relevanten Artikel der DS-GVO im Einzelnen dargelegt und ausführlich beschrieben. Weiterhin befasst sich Teil 1 mit den Begrifflichkeiten und Besonderheiten. Im Besonderen werden die Ziele des Datenschutzes und der Umgang mit den personenbezogenen Daten betrachtet. Des Weiteren werden die Bereiche der Haftung, Rechtbehelfe sowie Sanktionen beleuchtet. Da es bei Datenschutzverstößen zu erheblichen Bußgeldern kommen kann, wird dieser Abschnitt ebenfalls in Teil 1 ausführlich und verständlich beschrieben.

Teil 2 der Arbeit beschäftigt sich mit einer praktischen Umsetzung der Datenschutz-Grundverordnung. Hierbei geht es im Kern um die tatsächliche Implementierung der Datenschutz-Grundverordnung in ein Unternehmen. Dabei werden alle relevanten Abteilungen sowie die entsprechenden Besonderheiten hinsichtlich einer praktischen Umsetzung beleuchtet. Im Einzelnen werden technische als auch administrative Bereiche betrachtet und dargelegt. Eine Umsetzung im „laufenden“ Betrieb kann nicht problemlos durchgeführt werden. Aus diesem Grund werden Betrachtungen hinsichtlich der strukturellen Gegebenheiten ebenfalls beleuchtet. Dabei spielen Elemente aus dem Bereich des Change-Management ebenso eine Rolle wie die des Datenschutzes im Arbeitsverhältnis. Dabei ist der Aufbau sowie die Analyse eines umfangreichen Datenschutzmanagementsystems ebenso bedeutsam wie die länderübergreifenden Besonderheiten hinsichtlich eines Konzerndatenschutzes. Das Thema, Datenschutz und Compliance-Risiken, wird hinsichtlich möglicher Risiken ebenfalls in Teil 2 behandelt.

Teil 3 beinhaltet Handlungsempfehlungen an die Bereiche der Geschäftsführung, IT / Technik sowie der Personalabteilung. Dabei werden aktuelle Verstöße aufgeführt und deren Hintergründe betrachtet. Auf Grundlage ausgestellter Bußgeldbescheide werden die Ursachen, die zu den Bußgeldern geführt haben, dargelegt. Das hochaktuelle Thema der Covid-19 Pandemie und der damit verbunden Brisanz hinsichtlich einer möglichen Aufweichung des Datenschutzes ist ebenfalls Bestandteil des dritten Teils.

Schlüsselwörter: Personenbezogene Daten, Datenschutz, Datenschutz-Grundverordnung, Datenschutzrecht, Grundrechte, Recht auf Privatsphäre, Arbeitnehmerschutz, Changemanagement, Risikomanagement.

IV. Abstract „English“

The following paper describes in three parts the introduction of the **G**eneral **D**ata **P**rotection **R**egulation (**GDPR**). A variant for implementing the requirements of the General Data Protection Regulation introduced on 25 May 2018 is also presented. In the first part, the relevant articles of the GDPR are presented and described in detail. Part 1 also deals with terminology and special features. In particular, the objectives of data protection and the handling of personal data are considered. In addition, the areas of liability, legal remedies, and sanctions are examined. Since data protection violations can result in substantial fines, this section must also be explained in detail and in an understandable way, which is done on a theoretical basis, in Part 1 of this thesis.

Part 2 deals with a practical implementation of the General Data Protection Regulation. This is basically about the actual implementation of the General Data Protection Regulation in a company. All relevant departments as well as the corresponding particularities regarding a practical implementation are illuminated. In detail, both technical and administrative areas are considered and explained. An implementation in "running" operations cannot be carried out without problems. For this reason, considerations regarding the structural conditions are also illuminated. Elements from the area of change management play a role here, as do those of data protection in the employment relationship. The development and analysis of a comprehensive data protection management system are just as important as the special international features of Group data protection. The topic of data privacy and compliance risks is also dealt with in Part 2 regarding possible risks.

Part 3 contains recommendations for action to be taken by the Management Board, IT / Technology, and Human Resources. Current infringements are listed, and their background is considered. The reasons that led to the fines are explained based on the notices of fines issued. The highly topical subject of the Covid-19 pandemic and the associated explosiveness regarding a possible weakening of data protection is also described of the third Part.

Keywords: Personal Data, Data Protection, General Data Protection Regulation, Data Protection Law, Fundamental Rights, Right to Privacy, Employee Protection, Change Management, Risk Management.

V. Abbildungsverzeichnis

VI. Abkürzungsverzeichnis

A

a.A. ..... andere(r) Ansicht/Auffassung

ABl. ..... Amtsblatt

ABl. L ..... Amtsblatt der Europäischen Union, Teil L: Rechtsvorschriften

Abs. ..... Absatz

Abschn. ..... Abschnitt

Abt. ..... Abteilung

ADV ..... Auftragsdatenverarbeitung

AEUV ..... Vertrag über die Arbeitsweise der Europäischen Union

a.F. ..... alte Fassung

AG ..... Aktiengesellschaft, Amtsgericht

AGG ..... Allgemeines Gleichbehandlungsgesetz

AGB ..... Allgemeine Geschäftsbedingungen

allg. ..... allgemein

Alt. ..... Alternative

a.M. ..... andere Meinung

amtl. ..... amtlich

Anl. ..... Anlage

Anm. ..... Anmerkung(en)

AO. ..... Abgabenordnung

ArbG ..... Arbeitsgericht

Art. ..... Artikel

AT ..... Allgemeiner Teil

AuA ..... Arbeit und Arbeitsrecht (Zeitschrift)

Aufl. ..... Auflage

AuR ..... Arbeit und Recht (Zeitschrift)

Az. ..... Aktenzeichen

B

BAG ..... Bundesarbeitsgericht

BAGE ..... Entscheidungssammlung des Bundesarbeitsgerichts

Bay ..... Bayern

BayDSG ..... Bayerisches Datenschutzgesetz

BayLDA ..... Bayerisches Landesamt für Datenschutzaufsicht

BB ..... Der Betriebs-Berater (Zeitschrift)

BBG ..... Bundesbeamtengesetz

BbgDSG ..... Brandenburgisches Datenschutzgesetz

BCR ..... Binding Corporate Rules

Bd. ..... Band

BDI ..... Bundesverband der Deutschen Industrie

BDSG ..... Bundesdatenschutzgesetz

Begr. ..... Begründung

Beil. ..... Beilage

Beschl. ..... Beschluss

BetrVG ..... Betriebsverfassungsgesetz

BfDI ..... Bundesbeauftragte(r) für den Datenschutz und die Informationsfreiheit

BFH ..... Bundesfinanzhof

BGB ..... Bürgerliches Gesetzbuch

BGBl. ..... Bundesgesetzblatt

BGH ..... Bundesgerichtshof

BGHZ ..... Entscheidungssammlung des Bundesgerichtshofs in Zivilsachen

BMAS ..... Bundesminister(ium) für Arbeit und Soziales

BMG ..... Bundesmeldegesetz

BND ..... Bundesnachrichtendienst

BNDG ..... Gesetz über den Bundesnachrichtendienst

BRD ..... Bundesrepublik Deutschland

BRRG ..... Beamtenrechtsrahmengesetz

bspw. ..... beispielsweise

BVerfG ..... Bundesverfassungsgericht

BVerfGE ..... Entscheidungssammlung des Bundesverfassungsgerichts

BVerfSchG ..... Bundesverfassungsschutzgesetz

BVerwG ..... Bundesverwaltungsgericht

BVerwGE ..... Entscheidungssammlung des Bundesverwaltungsgerichts

bzgl. ..... bezüglich

bzw. ..... beziehungsweise

BYOD ..... Bring Your Own Device

C

CRM ..... Customer Relationship Management

CR ..... Computer und Recht (Zeitschrift)

D

DB ..... Der Betrieb (Zeitschrift)

ders. ..... derselbe

DFÜ ..... Datenfernübertragung

d.h. ..... das heißt

dies. ..... dieselbe

diesbzgl. ..... diesbezüglich

DSB ..... Datenschutzbeauftragter, Datenschutzberater (Zeitschrift)

DSFA ..... Datenschutz-Folgenabschätzung

DSG ..... Datenschutzgesetz

DS-GVO/DS-GVO ..... Datenschutz-Grundverordnung

DSK ..... Konferenz der unabhängigen Datenschutzbehörden
..... des Bundes und der Länder

DS-RL ..... Datenschutzrichtlinie (RL 95/46/EG)

DuD ..... Datenschutz und Datensicherung (Zeitschrift)

DVO ..... Durchführungsverordnung

E

EU-DSA ..... Europäischer Datenschutzausschuss

EG ..... Europäische Gemeinschaft(en)

EG-Vertrag ..... Vertrag zur Gründung der Europäischen Gemeinschaft vom 25.03.1957

Einl. ..... Einleitung

entspr. ..... entspricht, entsprechend

ErwGr, EG ..... Erwägungsgrund

EstG ..... Einkommenssteuergesetz

et al. ..... und andere

etc. ..... et cetera (und so weiter)

EU ..... Europäische Union

EuGH ..... Europäischer Gerichtshof

e.V. ..... eingetragener Verein

evtl. ..... eventuell

EWG ..... Europäische Wirtschaftsgemeinschaft

F

f. ..... folgende

ff. ..... fortfolgende

Fn. ..... Fußnote

G

GBl. ..... Gesetzblatt

gem. ..... gemäß

GG ..... Grundgesetz

ggf. ..... gegebenenfalls

GmbH ..... Gesellschaft mit beschränkter Haftung

GRCh ..... Charta der Grundrechte der Europäischen Union

GRUR ..... Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)

GVO ..... Grundverordnung

H

Halbs. / HS..... Halbsatz

HGB..... Handelsgesetzbuch

h.M. ..... herrschende Meinung

Hrsg. ..... Herausgeber

I

i.d.F. ..... in der Fassung

i.d.R. ..... in der Regel

IFG ..... Informationsfreiheitsgesetz

insb. ..... insbesondere

i.R.d. ..... im Rahmen des/der

i.S.d. ..... im Sinne des/der

IT ..... Informationstechnik

ITRB ..... Der IT-Rechts-Berater (Zeitschrift)

i.V.m. ..... in Verbindung mit

J

JI-RL ..... Richtlinie (EU) 2016 / 680 des Europäischen Parlaments und des Rates
..... vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung
..... personenbezogener Daten durch die zuständigen Behörden zum
..... Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung
..... von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr
..... und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

JZ ..... Juristenzeitung (Zeitschrift)

K

Kap. ..... Kapitel

krit. ..... Kritisch

KunstUrhbG..... Kunst Urhebergesetz

L

LAG ..... Landesarbeitsgericht

LAN ..... Local Area Network

LDSG ..... Landesdatenschutzgesetz

LG ..... Landgericht

lit. ..... litera

Ls ..... Leitsatz

LSG ..... Landessozialgericht

N

Nachw. ..... Nachweise

Nds. ..... Niedersachsen

n.F. ..... neue Fassung

NJW ..... Neue Juristische Wochenschrift (Zeitschrift)

Nr. ..... Nummer

NRW ..... Nordrhein-Westfalen

O

OLG ..... Oberlandesgericht

OVG ..... Oberverwaltungsgericht

P

PinG ..... Privacy in Germany (Zeitschrift)

R

RdA ..... Recht der Arbeit (Zeitschrift)

RDV ..... Recht der Datenverarbeitung

RegE ..... Regierungsentwurf

RFID ..... Radio Frequency Identification

RL ..... Richtlinie

RN/Rn. ..... Randnummer(n)

S

S. ..... Seite(n), Satz

sog. ..... sogenannt

ständ. ..... ständig

StGB ..... Strafgesetzbuch

StPO ..... Strafprozessordnung

str. ..... streitig, strittig

T

TB ..... Tätigkeitsbericht

teilw. ..... teilweise

TKG ..... Telekommunikationsgesetz

TMG ..... Telemediengesetz

TOM ..... Technische Organisatorische Maßnahme

U

u.a. ..... und andere, unter anderem

ULD ..... Unabhängiges Landeszentrum für Datenschutz

Urt. ..... Urteil

usw. ..... und so weiter

u.U. ..... unter Umständen

V

v. ..... vom, von

Var. ..... Variante

Verf. ..... Verfasser, Verfassung, Verfahren

VerfG ..... Verfassungsgericht

VerfGH ..... Verfassungsgerichtshof

VG ..... Verwaltungsgericht

VGH ..... Verwaltungsgerichtshof

W

WLAN ..... Wireless Local Area Network

WP ..... Working Paper

WWW ..... World Wide Web

Z

z.B. ..... zum Beispiel

ZD ..... Zeitschrift für Datenschutz

Ziff. ..... Ziffer

z.T. ..... zum Teil

VII. Einleitung

Beim Thema Datenschutz scheiden sich immer noch die Geister. Die Haltung umfasst aktuell alle Zustände, von der vollständigen Ablehnung bis zur Akzeptanz der Notwendigkeit eines adäquaten Datenschutzes aufgrund geänderter technischer Betrachtung. Die nachfolgende Arbeit beschäftigt aus diesem Grund mit der Einführung der Datenschutz-Grundverordnung und möglichen Folgen für ein Unternehmen. Das Thema kann aufgrund seiner Komplexität nicht autark betrachtet werden und erfordert somit eine Brücke zum Bereich des Managements. Aus Sicht eines Unternehmens, kommt es darauf an, nicht nur stur die Anforderungen einer Datenschutz-Grundverordnung umzusetzen, sondern auf die Summe aller Punkte bei der Erstellung eines angemessenen Datenschutz-Managementsystems. Ohne die Unterstützung des Managements ist es sehr unwahrscheinlich, dass die Datenschutz-Grundverordnung in einer Organisation erfolgreich umgesetzt werden kann. Denn die meisten Schritte dir für eine Umsetzung der Datenschutz-Grundverordnung erforderlich sind, können nur durchgeführt werden, wenn hierfür ein entsprechendes Budget bereitgestellt wird und andere Abteilungen den Umsetzungsprozess unterstützen.[1]

Der oder die LeiterInnen der IT / Technik ist ebenfalls nicht in der Lage die Datenschutz-Grundverordnung ohne Unterstützung umzusetzen. Der technische Apparat ist in der heutigen Zeit so umfangreich geworden und verändert sich darüber hinaus fast täglich. Die Sicherheit der IT-Infrastruktur spielt für Unternehmen eine essenzielle Rolle. Durch die weiter zunehmende Digitalisierung und Vernetzung der Unternehmen nach innen und außen erhöht sich die Gefährdungslage deutlich. Dabei entwickeln sich sowohl die Angriffsmethoden als auch die rechtlichen Rahmenbedingungen stetig weiter und stellen die Anwender vor umfangreiche Herausforderungen. Neben den steigenden Anforderungen an die IT-Sicherheit wurden gleichzeitig die Datenschutzvorschriften insbesondere durch die Einführung der Datenschutz-Grundverordnung (DS-GVO) weiter verschärft. Dies hat zur Folge, dass Unternehmen zur Gewährleistung der IT-Sicherheit

1 *Feiler/Horn,* Umsetzung der DSGVO in der Praxis, 2018, S. 3, Schritt 1 - Unterstützung aus dem Management sichern.

einer hohen Rechtfertigungspflicht unterliegen, insbesondere was die anlasslose Verarbeitung von personenbezogenen Daten anbelangt.[2]

Die Datenschutz-Grundverordnung fordert geeignete technische und organisatorische Maßnahmen durchzuführen, die eine erfolgreiche und ohne Zweifel strukturierte IT bzw. Technik gewährleistet. In diesem Zusammenhang wird gerne über „Privacy by Default" und „Privacy by Design" gesprochen. Hierbei handelt es sich um sogenannte technische Voreinstellungen bzw. Anwendungen, die im Idealfall die Datenschutz-Grundverordnung erfüllen können. Problematisch kann die Technikgestaltung dahingehend sein, dass eine hohe Anzahl möglicher Verfehlungen in Technikbereich ebenfalls mit einem Bußgeld belegt werden kann. Es handelt sich bei adäquater Technikgestaltung um eine große Investition, entsprechend dem Zustand der aktuellen Technik.

Der EuGH hat in seinem Urteil C-673/17 festgelegt, dass das Setzen von Cookies eine eindeutige Einwilligung des Internetnutzers erfordert. Ein voreingestelltes Ankreuzkästchen genüge in diesen Fällen nicht. Der EuGH stellt hier klar, dass die Einwilligung für jeden konkreten Fall erteilt werden muss. Weiterhin wurde ausgeführt, dass der Diensteanbieter gegenüber dem Nutzer in Bezug auf die Cookies, Angaben zur Funktionsdauer und zur Zugriffsmöglichkeit Dritter machen muss.[3] Somit ist erneut Bewegung in das Thema der Betreibung einer Webseite gekommen. Webseitenbetreiber müssen sich der aktuellen Gesetzeslage unterwerfen und die höchstrichterlichen Urteile umsetzen. Ergänzend ist anzuführen, dass die ePrivacy-Verordnung mit der Einführung der Datenschutz-Grundverordnung ebenfalls hätte umgesetzt werden müssen. Die ePrivacy-Verordnung ist aktuell für das Jahr 2020 geplant und muss hinsichtlich der datenschutzrechtlichen Bewertung beachtet werden.

Durch eine zunehmende Globalisierung ist die Arbeitswelt ebenfalls einem großen Wandel unterzogen. Dabei werden die Beschäftigungsbedingungen aufgrund von technischem und gesellschaftlichem Wandel stark geprägt. Beschäftigte stehen typischerweise in einem besonderen Abhängigkeitsverhältnis zum Arbeitgeber. Dies erfordert einen besonderen Schutz z. B. bei der Frage, wie freiwillig agiert ein

2 *Walter,* Datenschutz im Betrieb - DS-GVO in der Personalarbeit, 2018, S. 309, Abschnitt 21.1 - Ausgangslage.

3 EuGH, 01.10.2019 – C-673/17 http://curia.europa.eu/juris/.

Beschäftigter überhaupt, wenn er in die Verarbeitung personenbezogener Daten durch den Arbeitgeber einwilligt.

Andererseits sind gerade Arbeitgeber regelmäßig darauf angewiesen, sogar sehr persönliche Daten der Beschäftigten zu verarbeiten, um das Beschäftigungsverhältnis überhaupt begründen, durchführen oder beenden zu können. Dies hat es notwendig gemacht, den Umgang mit personenbezogenen Daten im Beschäftigungsverhältnis ergänzend zu den allgemeinen datenschutzrechtlichen Vorschriften besonders zu regeln (siehe. Beschäftigtendatenschutz).[4]

Nach dem Inkrafttreten der DS-GVO sind Verstöße gegen den Beschäftigtendatenschutz und diesbezügliche Anweisungen der Aufsichtsbehörden nunmehr mit ungleich drastischeren Geldbußen belegt als noch zu Zeiten davor. Arbeitgeber, die natürliche Personen sind, drohen Geldbußen von bis zu 20 Mio. EUR, Unternehmen sogar in Höhe von bis zu 4 Prozent ihres weltweiten Umsatzes, wenn dieser Betrag höher ist. Dabei handelt es sich um Maximalbeträge, die natürlich auch deutlich geringer ausfallen können.[5]

Dieses hat unweigerlich zur Folge, dass sich die Unternehmen und deren Geschäftsmodelle einem Veränderungsprozess unterziehen müssen. Diese Punkte des Beschäftigtendatenschutzes müssen aus den genannten Gründen ebenfalls einer Betrachtung unterzogen werden.

Die Datenschutz-Grundverordnung wird als Daten- und Persönlichkeitsschutz verstanden. Der Schutz persönlicher Daten hat in allen Bereichen oberste Priorität. Dabei ist der extreme Anstieg an verarbeiteten Daten in allen Bereichen, soweit möglich, zu betrachten. Die Menge der jährlich verarbeiteten Daten steigt weltweit in nie dagewesene Höhen. Lag die Datenmenge im Jahr 2018 noch bei 33 Zettabyte (1 Zettabyte = 1,099512 x 10^{12} Gigabyte), wird für das Jahr 2025 bereits mit einer

4 *Buhl et al.,* Der erwachte Gesetzgeber, 2017, S. 97.
5 *Walter,* Datenschutz im Betrieb - DS-GVO in der Personalarbeit, 2018, Seite 118, Abschnitt 6.10 Abs. 1.

Datenmenge von 175 Zettabyte gerechnet.[6] Diese **Datenflut** muss reguliert und in angemessener Weise Prüfungen unterzogen werden.

Diese Menge an Daten wird allgemein als Big Data bezeichnet. Mit Big Data werden große Mengen an Daten bezeichnet, die u.a. aus Bereichen wie Internet und Mobilfunk, Finanzindustrie, Energiewirtschaft, Gesundheitswesen, Verkehr und aus Quellen wie intelligenten Agenten, sozialen Medien, Kredit- und Kundenkarten, Smart-Metering-Systemen, Assistenzgeräten, Überwachungskameras sowie aus Flug- und Fahrzeugdaten stammen und die mit speziellen Lösungen zu zwecken der (Inter-) Dependenzanalyse, Umfeld und Trendforschung sowie zu Systemen und Produktionssteuerungszwecken gespeichert, verarbeitet und ausgewertet werden.[7]

Die Vorstellung der Steuerung technischer Entwicklung durch das Datenschutzrecht wird sich allerdings nur bedingt umsetzen lassen. Vielmehr ist anzunehmen, dass die technischen Entwicklungen auch in der Zukunft neue Herausforderungen für die Gewährleistung des Betroffenenschutzes durch das Datenschutzrecht schaffen werden.[8]

Die EU-Datenschutz-Grundverordnung (DS-GVO) hat mit Wirkung zum 25.5.2018 ein in weiten Teilen einheitliches und in allen Mitgliedstaaten der Europäischen Union unmittelbar anwendbares Datenschutzrecht geschaffen. Es enthält substanzielle Änderungen, namentlich etwa mit Blick auf umfangreiche Betroffenenrechte, eine völlige Neuausrichtung der Datenschutzaufsicht und die deutlich erweiterte Möglichkeit, hohe Bußgelder von bis zu 4 Prozent des Vorjahresumsatzes der Unternehmen zu verhängen. Neben den harmonisierten Regelungen werden bestimmte Bereiche, wie zum Beispiel der Beschäftigtendatenschutz, die Zulässigkeit der Datenverarbeitung der öffentlichen Stellen und eine Reihe weiterer Bereiche in unterschiedlichem Ausmaß den Gesetzgebern der Mitgliedstaaten zur Regelung überlassen.[9]

Datenschutz in der Europäischen Union und im Europäischen Wirtschaftsraum einheitlich zu gewährleisten, ist vor allem Sache der unabhängigen Aufsichtsbehörden.

---

6 *Statista GmbH,* Prognose zum weltweit generierten Datenvolumen 2025,, https://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/#professional.

7 *Caldarola/Schrey,* Big Data und Recht, 2019, S. 1, Rn. 1 Abs. 1.

8 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, S. 4, Rn. 3.

9 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 40 von 87533.

Sie erhalten hierfür neue Aufgaben und Befugnisse, Pflichten zur Zusammenarbeit sowie Institutionen und Verfahren der einheitlichen Willensbildung. Diese Neuerungen verändern die Rolle und den Charakter der unabhängigen Aufsichtsbehörden und verursachen einen zusätzlichen Ressourcenbedarf. Um über die neuen Aufgaben und die zusätzlichen Bedarfe Klarheit zu gewinnen, beauftragten die unabhängigen Aufsichtsbehörden der Länder den Autor, in einem Rechtsgutachten den zusätzlichen Aufwand zu bewerten, der sich für die Datenschutzbehörden der Länder aus dem Inkrafttreten der Datenschutz-Grundverordnung gegenüber der bisherigen Rechtsanwendung ergibt. Dabei sollte sowohl die Vorbereitungszeit seit Inkrafttreten der Verordnung am 24. Mai 2016 bis zur Geltung der Verordnung in den Mitgliedstaaten ab dem 25. Mai 2018 als auch die nachfolgende Zeit, wenn die Verordnung in allen Mitgliedstaaten gilt, berücksichtigt werden.[10]

Die „Bitcom Research GmbH“ veröffentlichte im September 2019 eine Studie über den Erfolg bei der Umsetzung der Datenschutz-Grundverordnung. Demnach kämpft die deutsche Wirtschaft immer noch mit der Umsetzung der Datenschutz-Grundverordnung. Fast eineinhalb Jahre nach Geltungsbeginn haben zwar zwei Drittel der Unternehmen (67 %) die neuen Datenschutzregeln **mindestens zu großen Teilen umgesetzt**. Dabei hat allerdings **erst ein Viertel** (25 %) die Umsetzung der DS-GVO **vollständig abgeschlossen**. Das ist das Ergebnis einer repräsentativen Befragung unter mehr als 500 Unternehmen aus Deutschland, die der Digitalverband Bitkom im Rahmen seiner Privacy Conference vorgestellt hat. Weitere 24 Prozent haben die Verordnung teilweise umgesetzt, 6 % stehen noch am Anfang. Rechtsunsicherheit und ein schwer abzuschätzender Umsetzungsaufwand sind für jeweils zwei Drittel der Unternehmen (68 %) die größten Herausforderungen. Mehr als die Hälfte (53 %) beklagen fehlende Umsetzungshilfen, gut ein Drittel (37 %) sieht fehlendes Fachpersonal als größte Herausforderung. Über 97% sehen den größten Aufwand in der Umsetzung der aufwendigen Dokumentation. Die Katalogisierung der Prozesse ist für 93 % sehr aufwändig, 86 % geben dies für ihr Vertragsmanagement an. Die sogenannten **Privacy-by-Design**-Anforderungen zu erfüllen, bedeutet für 84 % viel Arbeit. Ähnlich viele (82 %) kämpfen wegen der Datenschutz-Grundverordnung mit hohen Aufwänden für den

10 *Roßnagel,* Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, 2017, S. 1 Abs. 2.

Betrieb ihrer Webseiten. Nicht nur der Aufwand ist hoch. Für viele haben die Datenschutzregeln auch enge Grenzen für Innovationen gesetzt. Jedes siebte Unternehmen (14 %) erklärt: In unserem Unternehmen sind neue, innovative Projekte aufgrund der Datenschutz-Grundverordnung gescheitert.[11]

Mögliche Ursachen für die nicht vollumfänglich umgesetzte Datenschutz-Grundverordnung kann die mit Einführung der Datenschutz-Grundverordnung angekündigte und noch ausstehende ePrivacy-Verordnung sein. Die ePrivacy-Verordnung ist ebenfalls eine Verordnung, die unverzüglich umgesetzt werden muss. Die ePrivacy-Verordnung enthält Anforderungen an den Datenschutz, welche in der Datenschutz-Grundverordnung nicht ausdrücklich geregelt wurden. Diese Unsicherheit spiegelt sich selbstverständlich in der Bereitschaft die Datenschutz-Grundverordnung komplett umzusetzen wider.

Die Flash Eurobarometer-Umfrage von 2003 über Unternehmenspraktiken hat deutlich gemacht, dass die Einhaltung der geltenden Informationspflichten ein Problem darstellt. Die Unternehmen gaben zu, dass sie den betroffenen Personen nicht immer die gesetzlich vorgeschriebenen Informationen mitteilen und sich somit nicht immer an die Datenschutzvorschriften halten. Lediglich 37 % der Unternehmen teilen den betroffenen Personen die Identität des für die Verarbeitung Verantwortlichen mit und nur 46 % informieren die betroffenen Personen über den Zweck der Erhebung.[12]

Es sind derartige Informationen, die eine genaue Betrachtung hinsichtlich der rechtlichen Anforderungen sowie den Besonderheiten bei der Umsetzung der Datenschutz-Grundverordnung, erfordern. Der erste Teil, der aus insgesamt drei Teilen bestehenden Thesis, soll aus diesem Grund die theoretische Grundlage für eine Einführung der Europäischen Datenschutz-Grundverordnung legen. Im ersten Teil werden darüber hinaus die wichtigsten Punkte erläutert. Die Datenschutz-Grundverordnung gliedert sich aktuell in 11 Kapitel, die alle 99 Artikel behandeln. Weiterhin werden die 173 Erwägungsgründe der neuen Verordnung erläutert sowie die Unterschiede zum „alten“

11 *Bitcom Research GmbH*, Zwei Drittel der Unternehmen haben DS-GVO größtenteils umgesetzt, Berlin 17.09.2019, https://www.bitkom-research.de/de/pressemitteilung/zwei-drittel-der-unternehmen-haben-ds-gvo-groesstenteils-umgesetzt.

12 *Lukas* (Hrsg.), Gesetzbuch Datenschutzrecht, S. 356, Stellungnahme WP 100 (Informationspflichten).

BDSG. 51 Artikel regeln das materielle und 48 das formelle, organisatorische und kompetenzrechtliche Datenschutzrecht.[13]

Des Weiteren werden die Grundlagen des Datenschutzes ausführlich betrachtet, wie auch die Rechtsgeschichte des Datenschutzes beleuchtet. Da die Begrifflichkeiten nicht, wie in der Datenschutz-Grundverordnung gefordert, in besonders einfacher, klarer und verständlicher Sprache formuliert sind, müssen diese ausführlich betrachtet und unmissverständlich erläutert werden. Mit der neuen Datenschutz-Grundverordnung 2016 / 679 vom 27.04.2016 kommt das Datenschutzrecht in neuer Gestalt daher, insbesondere der Geltungsbereich der Datenschutz-Grundverordnung.

Das „Recht am eigenen Bild“, wird in vielen Publikationen oft erwähnt, aber in der Datenschutz-Grundverordnung nicht wörtlich wiedergegeben. Gleiches gilt für das „Recht auf Vergessen“ werden. So oft zitiert bilden sie doch Kernaussagen ab, welche in Zusammenhang mit der Europäischen Datenschutz-Grundverordnung betrachtet werden müssen.

Es wurden viele literarische Quellen angekündigt, aktualisiert und einige wurden vor Einführung der DS-GVO bereits publiziert. Schwierig war in diesem Fall die Ungewissheit, welche die Einführung und die möglichen Konsequenzen betreffen können. In der Folge wurden Lehrgänge, juristischer Beistand durch spezialisierte Kanzleien, externe Unternehmen, die eine Einführung begleiten wollten, sowie weitere Unterstützung angeboten. Schwierig war in diesem Zusammenhang eine adäquate Planung bzw. Übersicht zu erhalten, die alle erforderlichen Bereiche vollumfänglich betrachteten und unternehmenskonform umsetzen konnten.

Der zweite Teil beschäftigt sich mit der Einführung, den organisatorischen Themen sowie den erforderlichen Auflagen. Hierbei geht es um die tatsächliche Implementierung der Datenschutz-Grundverordnung. Dabei wird unter anderem die Frage zu beantworten sein: „ist eine praktische Umsetzung mit den gegebenen Mitteln möglich und sind Schwachstellen in der Datenschutz-Grundverordnung erkennbar?“. Des Weiteren müssen einzelne Unternehmensbereiche an die geänderten Umstände angepasst werden, was ebenfalls durch eine Betrachtung im Abschnitt, Change-Management, dargelegt wird.

---

13 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Taeger/Schmidt, S. 16, Rn. 34, S. 2.

Je nach Unternehmensgröße ist ein externer oder interner Datenschutzbeauftragter zu benennen oder zu beauftragen. Die neue Datenschutz-Grundverordnung hat auch hierzu Änderungen generiert, die eine Entscheidung bezüglich interner und oder externer Wahl nicht eben einfacher gestalten. Da sich das Aufgabengebiet sowie die Haftung erheblich geändert haben, müssen diese Punkte detailliert betrachtet werden. Bei dem in der Folge beschriebenen Unternehmen handelt es sich um eine Ländergesellschaft, welches an einen internationalen Konzern angeschlossen ist. Dieser Umstand erfordert es, dass die konzernübergreifenden Datenübertragungen ebenfalls zu betrachten sind, wie auch die eigentliche Struktur eines Konzernes und den damit verbundenen Auflagen.

Der Konzerndatenschutz hat stetig an Brisanz hinzugewonnen. Die technischen Möglichkeiten sind heute ausgereifter und kostengünstiger als noch vor einigen Jahren, zumal sich die Vernetzung innerhalb der Konzerne, deutlich erhöht hat. Outsourcing der IT-Leistungen ist eine viel diskutierte Möglichkeit, um kostengünstiger agieren zu können. Dabei gilt immer auch die Betrachtung der tatsächlichen Einsparungen bei gleichzeitigem Einflussverlust. Cloud-Computing verspricht einfachen kostengünstigen Datenzugriff und Funktionen. Wie verhält es sich mit dem Datenschutz bei Cloud-Software-Anbieter die im Ausland (ebenfalls außerhalb des europäischen Auslands) ihren ständigen Sitz haben? Die Diskussion zum Konzernprivileg betrifft inzwischen vor allem die Frage, wie Konzerne mit impraktikabler Regelung des Fehlens eines Privilegs umgehen und rechtkonform handeln können.[14]

Der dritte Teil beschäftigt sich unter anderem mit den Empfehlungen / Auswirkungen auf das in dieser Arbeit beschriebene Thema. Da alle drei Teile die gesamte Thesis darstellen, werden vorab die Hintergründe sowie die Entwicklung des Datenschutzes umfänglich beleuchtet. Darüber hinaus werden die einzelnen Tätigkeiten mit den erforderlichen Daten betrachtet, da diese autark als Nachschlagewerk verwendet werden können. Abschließend werden Empfehlungen ausgesprochen, die folgende Abteilungen betreffen:

- Geschäftsleitung
- IT / Technik
- Personal

[14] *Lachenmann,* Datenübermittlung im Konzern, 2016, S.2, Abs.3.

Datenschutzbeauftragte(n) / Verantwortliche(n) eines Unternehmens, sei es nun eine externe oder interne Variante, benötigen adäquate Empfehlungen mit Hinweisen, die für die Durchführung der Tätigkeiten in Teilen erforderlich sind. Aufgrund der Komplexität des Themas ist eine kurze Übersicht über das Thema der verhängten Bußgelder ebenfalls aufgelistet und soweit möglich einer Analyse unterzogen. Diese werden im dritten Teil ebenfalls dargestellt.

Das in der Folge beschriebene Unternehmen wurde im Jahr 2018 durch einen europäischen Mitbewerber mit weiteren Ländergesellschaften käuflich erworben. Das Unternehmen sollte unter den aktuellen Gegebenheiten mit den bestehenden Strukturen weitergeführt werden.

Als eine unternehmerische Entscheidung wurde der Verkaufsprozess bereits Anfang 2018 initiiert. In der Folge konnten lediglich einige gesetzlichen Anforderungen der Datenschutz-Grundverordnung umgesetzt werden. Alle weiteren Thesen sowie die Erfahrungen aus der Anwendung der Datenschutz-Grundverordnung konnten nicht ausreichend betrachtet werden und wurden in der Folge auf theoretischer Basis erstellt.

Weiterhin werden elf aktuelle Bescheide zum Thema Bußgeld und Datenschutz aufgeführt und erläutert. Abschließend sind Muster-Vorlagen zu den Themen, technisch organisatorische Maßnahmen, Datenschutzerklärung, Betriebsvereinbarung sowie Datenschutzinformationen im Bewerbungsprozess im Anhang aufgeführt.

Es ist dem Verfasser nicht gestattet, Firmeninterna, Statistiken und oder Namen zu verwenden. Darüber hinaus sind alle Informationen, die den Verkauf bzw. Kauf, die Verhandlungen sowie Präsentationen betreffen, durch eine Verschwiegenheitserklärung geschützt und dürfen ebenfalls nicht Gegenstand der Thesis sein.

Bei der Erstellung und Formulierung der vorliegenden Arbeit wurde auf Genderneutralität Wert gelegt. In Fällen, in denen dieses nicht gelungen ist, wurde das generische Maskulinum oder eine neutrale Schreibweise verwendet.

Über Anregungen und Kritik bezüglich der vorliegenden Arbeit freue mich.

Teil. 1 - Grundlagen

1 Die Europäische Datenschutz-Grundverordnung

1.1 Allgemeine Informationen

Am 25. Mai 2018 wurde die Verordnung (EU) 2016 / 679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)[15] (ABI. L 119 vom 4.5.2016, S.1; L 314 vom 22.11.2016, S. 72) unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union. Ziel der Verordnung (EU) 2016 / 679 war es ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von Daten in allen Mitgliedstaaten (Erwägungsgrund 10) zu ermöglichen. Der Unionsgesetzgeber hatte sich für die Handlungsform einer Verordnung entschieden, damit innerhalb der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist (Erwägungsgrund 13). Die Verordnung (EU) 2016 / 679 sieht eine Reihe von Öffnungsklauseln für den nationalen Gesetzgeber vor. Zugleich enthält die Verordnung (EU) 2016 / 679 konkrete, an die Mitgliedstaaten gerichtete Regelungsaufträge. Daraus ergab sich gesetzlicher Anpassungsbedarf im nationalen Datenschutzrecht.[16] (BDSG - Bundesdatenschutzgesetz)

Darüber hinaus diente der vorliegende Gesetzentwurf der Umsetzung der Richtlinien (EU) 2016 / 680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr

15 Datenschutz Grundverordnung 2016 (27 April 2016).

16 *Gesetzentwurf der Bundesregierung, Drucksache 18/11325, Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes,* Drucksache 18/11325, Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU-DSAnpUG-EU),

und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates[17] (AB L 119 vom 04.05.2016, S. 89)[18], soweit die der Richtlinie unterfallenden Staaten nach deren Artikel 63 verpflichtet sind, bis zum 6. Mai 2018 die Rechts- und Verwaltungsvorschriften zu erlassen, die erforderlich sind, um dieser Richtlinie nachzukommen. Die Umsetzung der Richtlinie (EU) 2016 / 680 wird über die im vorliegenden Gesetzentwurf enthaltenen relevanten Regelungen hinaus auch noch gesondert im Fachrecht erfolgen.[19]

Im Interesse einer homogenen Entwicklung des allgemeinen Datenschutzrechts soll das neu gefasste Bundesdatenschutzgesetz, soweit nicht dieses selbst oder bereichspezifische Gesetze abweichende Regelung treffen, auch für die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten öffentlicher Stellen des Bundes Anwendung finden, die außerhalb des Anwendungsbereichs des Unionsrechts liegen, wie etwa die Datenverarbeitung durch das Bundesamt für Verfassungsschutz, den Bundesnachrichtendienst oder den Militärischen Abschirmdienst oder im Bereich des Sicherheitsüberprüfungsgesetzes. Dies geht einher mit zusätzlichem gesetzlichen Änderungsbedarf in den jeweiligen bereichsspezifischen Gesetzen.[20]

Die Richtlinie 95/46/EG wurde mit Wirkung vom 25.05.2018 aufgehoben.[21]

Erwägungsgrund 171

Die Richtlinie 95/46/EG[22] wurde durch diese Verordnung aufgehoben. Verarbeitungen, die zum Zeitpunkt der Anwendung dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden. Beruhen die Verarbeitungen auf einer Einwilligung gemäß der Richtlinie 95/46/EG, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht, so dass der Verantwortliche die Verarbeitung

17 IN ANWENDUNG VON TITEL VI DES EU-VERTRAGS ERLASSENE RECHTSAKTE, in: Amtsblatt der Europäischen Union,
18 Amtblatt L 119 59 Jahrgang (4. Mai 2016), S. 89.
19 Drucksache 18/11325.
20 Drucksache 18/11325.
21 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art 94 DSGVO.
22 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates.

nach dem Zeitpunkt der Anwendung der vorliegenden Verordnung fortsetzen kann. Auf der Richtlinie 95/46/EG beruhende Entscheidungen bzw. Beschlüsse der Kommission und Genehmigungen der Aufsichtsbehörden bleiben in Kraft, bis sie geändert, ersetzt oder aufgehoben werden.[23]

Art. 94 Abs. 1 DS-GVO regelt zeitgleich zum Geltungsbeginn der DS-GVO nach Art. 99 Abs. 2 die Aufhebung der RL 95/46/EG[24]. Ab diesem Zeitpunkt gelten Verweise auf die aufgehobene Richtlinie als Verweise auf die DS-GVO. Verweise auf die Art. 29-Datenschutzgruppe gelten als Verweise auf den Europäischen Datenschutzausschuss nach Art. 68 ff.[25]

23 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 171.

24 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates.

25 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).

1.2 Entwicklung des Datenschutzes

Die Entwicklung des Datenschutzes in Deutschland ist untrennbar verbunden mit der Entwicklung der automatisierten Datenverarbeitung ab Mitte des 20. Jahrhunderts. Das Arbeiten mit Karteisystemen und Lochkartenautomaten wurde fortlaufend zeitintensiver und unwirtschaftlich. Die stetig zunehmenden Aufgaben der öffentlichen Daseinsvorsorge und die Notwendigkeit der Kommunikation zwischen den Behörden machten es notwendig, in der öffentlichen Verwaltung EDV-Anlagen zum Einsatz zu bringen. Diese EDV-Anlagen wurden immer weiter ausgebaut und vernetzt, mit der Folge, dass Anfang der 70er Jahre bereits erste Rechenzentren in Betrieb genommen wurden. Etwaig daraus resultierende datenschutzrechtliche Sorgen waren in Bevölkerung und Medien aber noch nicht verbreitet.[26]

Von den Anfängen des Datenschutzes an hat sich die Kodifikation weiterentwickelt. Einige Grundmerkmale, vor allem das Verbreitungsverbot und der Schutz der Daten sind geblieben. Die Kodifikation, **BDSG 1977**[27] vom 1.2.1977, basierte in Grundzügen auf einem wissenschaftlichen Gutachten. Darin wurde nicht ein materielles Schutzgut als Kern einer zukünftigen Regelung zur Lösung vorgeschlagen, sondern die Regelung des Umgangs mit personenbezogenen Daten.[28]

In Deutschland wurde bereits unmittelbar nach Inkrafttreten des BSDG (1977) über eine Novellierung des Gesetzes nachgedacht. Im Januar 1980 wurde mit der Vorlage eines Gesetzesentwurfes zur Änderung des BDSG der Novellierungsprozess begonnen. Bis zur Verabschiedung des Änderungsprozesses vergingen 10 Jahre. Geprägt wurde der Gesetzesprozess von weiteren Änderungs- und Referentenentwürfen, sowie von dem sogenannten „Volkszählungsurteil“ des Bundesverfassungsgerichts vom 15.12.1983.[29]

Am 20.12.1990, fast genau sieben Jahre nach dem Volkszählungsurteil des BVerfG wurde das novellierte BDSG (1990) verkündet.[30] Zu diesem Zeitpunkt zeichnete sich

---

26 *Schläger/Thode* (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S.9, 1.3. / 22.
27 [Der Titel "BDSG_erste_Fassung_1977" kann nicht dargestellt werden. Die Vorlage "Fußnote - Zeitschriftenaufsatz - (Standardvorlage)" beinhaltet nur Felder, welche bei diesem Titel leer sind.]
28 *Forgó/Helfrich/Schneider* (Hrsg.), Betrieblicher Datenschutz, S. 4 -5.
29 *Moos* (Hrsg.), Datennutzungs- und Datenschutzverträge, S. 1617.
30 *Moos/Schefzig/Arning* in, De Gruyter Praxishandbuch (Seite 16, Rn. 18 Abs. 1, S. 16 und 17)17.

bereits ab, dass auch auf europäischer Ebene datenschutzrechtliche Regelungen für einen gemeinsamen Markt getroffen werden sollten. Nach mehreren Entscheidungen der Kommission, bereits in den Jahren 1975, 1976, 1979 und 1982 die den Willen beurkundeten, den Datenschutz auf europäische Ebene, Regeln zu wollen, legte die EG-Kommission im September 1990 und damit 2 Monate vor Verkündung des BDSG (1990) ein Vorschlagpaket für eine formelle europäische Datenschutzrichtlinie vor.[31] Nach fünfjähriger Diskussion wurde am 23 November 1995 die Richtlinie 95/46/EG des europäischen Parlaments und des Rates vom 24 Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DSRL) im Amtsblatt der Europäischen Union veröffentlicht.[32]

Es existieren durchaus auch kritische Stimmen zum Datenschutz und deren Umsetzung, beginnend mit dem BDSG aus dem Jahre 1977.

Ein Blick in die Vergangenheit und in die Zukunft zeigt drei durchgängige rote Fäden auf.

1. Das BDSG 1977 war unvollkommen, die DS-GVO und das ergänzende BDSG bleiben ebenfalls unvollkommen. Während der Gesetzgeber z.B. bei der Ausgestaltung des BGB auf die Erfahrungen insbesondere des römischen Rechts, aber auch der germanischen Rechte zurückgreifen konnte, gab es bezüglich der datenschutzrechtlichen Gesetzgebung kaum Erfahrungswerte. Das BDSG 1977 wurde quasi auf der „**grünen Wiese**“ gesetzt.
2. Das Gesetz war seit jeher selbst für Juristen schwer verständlich, die DS-GVO und dass sie ergänzende BDSG erschwert noch mehr das Verstehen. Dies liegt zum einen an der Materie, zum anderen an der Amtssprache der EU. Die Übersetzungen orientieren sich am englischen und französischen Sprachgebrauch[33]
3. Die datenschutzrechtlichen Regelungen wurden und werden auch weiterhin einäugig beurteilt – stets aus der Sicht des Betroffenen, der natürlichen Person, über die Daten gespeichert werden. Es ist zu begrüßen, dass Art. 1 DS-GVO dem

31 *Moos/Schefzig/Arning* in, De Gruyter Praxishandbuch (Seite 16, Rn. 18, Abs. 2).
32 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates.
33 *Erich-Schmidt-Verlag,* Datenschutz-Grundverordnung (DS-GVO), Bundesdatenschutzgesetz (BDSG), 2017, DS-GVO - Kommentar, 0200 Art. 1, S. 3, S. 4 Rn. 2a, Rn. 2.

Schutz natürlicher Personen gleichwertig des freien Verkehr solcher Daten gegenüberstellt (Abs.1) und dieses noch klarer in Abs. 3 formuliert: „Der freie Verkehr personenbezogener Daten darf … weder eingeschränkt noch verboten werden“. Dieses wird in den Diskussionen, aber auch in der Literatur (absichtlich oder unabsichtlich) meist nicht erwähnt.[34]

1.3 Rechtsakte: EU-Verordnung und Richtlinie

Nach Artikel 288 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) können die europäischen Institutionen fünf Arten von Rechtsakten verabschieden:

- die Verordnung;
- die Richtlinie;
- den Beschluss;
- die Empfehlung;
- die Stellungnahme.

Verordnungen, Richtlinien und Beschlüsse sind verbindliche Rechtsakte; Empfehlung und Stellungnahme sind dies nicht.[35]

1.3.1 Verordnungen

- haben „allgemeine Geltung“
- sind „in allen Teilen verbindlich“
- gelten „unmittelbar“ in jedem Mitgliedstaat.[36]

Verordnungen sind inhaltlich in allen ihren Teilen, nicht nur wie die Richtlinie, in Ihren Zielen verbindlich. Verordnungen haben per Definition unmittelbare Geltung, d.h. sie gelten direkt und ohne Einschränkungen für und gegen alle Normadressen. Sie sind Teil

34 *Erich-Schmidt-Verlag,* Datenschutz-Grundverordnung (DS-GVO), Bundesdatenschutzgesetz (BDSG), 2017, DS-GVO - Kommentar, 0200 Art. 1, S. 4, Rn. 3, Abs. 1.

35 *Amt für Veröffentlichungen*, EUR-Lex - ai0032 - EUR-Lex Datum der letzten Überprüfung: 08/09/2015.

36 *Vedder/Heintschel von Heinegg* (Hrsg.), Europäisches Unionsrecht, S. 1137, Rn. 16.

des in den Mitgliedstaaten geltenden Rechts. Sie bedürfen nicht etwa eines Zustimmungs- oder Umsetzungsaktes von Organen der Mitgliedstaaten.

Verordnungen gelten in jedem Mitgliedstaat und schaffen unionsweit einheitliches, identisches, in allen Mitgliedstaaten unabdingbar und gleichermaßen geltendes Recht.[37] Als Kehrseite ihrer unmittelbaren Geltung entfallen Verordnungen bei einem Austritt aus der Union mit dessen Wirksamwerden, sofern nicht durch nationale Gesetzgebung pauschal oder speziell ihrer weiteren Geltung als dann innerstaatliches Recht angeordnet wird.[38]

Zu betrachten ist in diesem Zusammenhang der Austritt des Vereinigten Königreichs, dessen (Br)Exit für den 31.01.2020, mit einer Übergangsfrist, von bis zu zwei Jahre nach dem offiziellen Austritt, geplant war. Bedingt durch die aktuelle Covid. 19 Pandemie wurde dieses Datum einvernehmlich verschoben. Es tun sich in diesem Zusammenhang einige Fragen, bezüglich der datenschutzrechtlichen Regelungen, auf. Bspw. welches Recht wird im Anschluss an den **Brexit** (**br**itischer **Exit**) zur Anwendung gelangen und was ist dabei im Besonderen zu beachten?

1.3.2 Richtlinien

Das strukturelle Vorbild der Richtlinie war das deutsche Rahmengesetz i.S.v. Art. 75 GG, das durch die Föderalismusreform von 2006 allerdings beseitigt worden ist. In einem zweistufigen Rechtsetzungsverfahren werden zunächst:

- Durch die Richtlinie die allein die Mitgliedstaaten als Normadressaten verpflichtet, wesentliche Regelungsinhalte festgelegt, die dann auf einer zweiten Stufe;
- In den Mitgliedstaaten in nationales Recht umgesetzt werden müssen;
- Erst das nationale Umsetzungsrecht ist für natürliche und juristische Personen verbindlich.[39]

Mit dem Rechtsformwechsel von der Datenschutz-Richtlinie zur Verordnung mit unmittelbar anwendbaren Regelungen (vgl. Art. 288 II EUV) soll die bereits unter der

37 *Vedder/Heintschel von Heinegg* (Hrsg.), Europäisches Unionsrecht, S.1138, Rn.18.
38 *Vedder/Heintschel von Heinegg* (Hrsg.), Europäisches Unionsrecht, Seite.1138, Rn.19.
39 *Vedder/Heintschel von Heinegg* (Hrsg.), Europäisches Unionsrecht, S. 1138, Rn. 21.

DSRL „grundsätzlich umfassende Harmonisierung“ fortgesetzt, die im Datenschutz bestehenden Unterschiede zwischen den Mitgliedstaaten weiter verringert und hierdurch das genannte Doppelziel erreicht werden.

Tatsächlich gestaltet sich die Datenschutz-Grundverordnung (DS-GVO) materiell aber als ein Hybrid **zwischen** Verordnung und Richtlinie, denn für zahlreiche Regelungen der DS-GVO kann gerade keine unmittelbare Anwendbarkeit festgestellt werden.[40]

1.3.3 Aufbau und Interpretation der DS-GVO

Die Datenschutz-Grundverordnung (DS-GVO) besteht aus 11 Kapitel mit insgesamt 99 Artikel.

Kapitel I Allgemeine Bestimmungen

(Art. 1 – Art. 4)

~~~~~~

Kapitel II Grundsätze

(Art. 5 – Art. 11)

~~~~~~

Kapitel III Rechte der betroffenen Person

(Art.12 – Art. 23)

~~~~~~

Kapitel IV Verantwortlicher und Auftragsverarbeiter

(Art. 24 – Art. 43)

~~~~~~

Kapitel V Übermittlung personenbezogener Daten an Drittländer oder an

internationale Organisationen

(Art. 44 – Art. 50)

40 AD Legendum AL 1/2018, 1 (AL 1/2018 – S.1-88, S.13).

~~~~~~

Kapitel VI Unabhängige Aufsichtsbehörden

(Art. 51 – Art. 59)

~~~~~~

Kapitel VII Zusammenarbeit und Kohärenz

(Art. 60 – Art. 76)

~~~~~~

Kapitel VIII Rechtsbehelfe, Haftung und Sanktionen

(Art. 77 – Art. 84)

~~~~~~

Kapitel IX Vorschriften für besondere Verarbeitungsfunktionen

(Art. 92 – Art. 93)

~~~~~~

Kapitel X Delegierte Rechtsakte und Durchführungsrechtsakte

(Art. 92 – Art. 93)

~~~~~~

Kapitel XI Schlussbestimmungen

(Art. 94 – Art. 99)

Die Artikel der Verordnung sind dabei immer auch im Zusammenhang mit den Erwägungsgründen (mögliche Abkürzungen sind: ErwGr oder EG.) zu verstehen. Anders als eine deutsche Gesetzesbegründung sind die Erwägungsgründe integraler Bestandteil der Verordnung. Dementsprechend empfiehlt sich bei der Lektüre der Verordnung immer auch die Prüfung, ob gegebenenfalls die Erwägungsgründe weitere Ausführungen zu bestimmten Pflichten oder Definitionen enthalten oder gelegentlich Themen nur in den Erwägungsgründen angesprochen sind (wie bspw. die Videoüberwachung in Erwägungsgrund. 91). In der Folge werden alle aktuellen sowie erforderlichen Erwägungsgründe immer in Verbindung mit den 173 Erwägungsgründen abgedruckt und auch verbunden.

Erwägungsgrund 91

Dies sollte insbesondere für umfangreiche Verarbeitungsvorgänge gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und - beispielsweise aufgrund ihrer Sensibilität - wahrscheinlich ein hohes Risiko mit sich bringen und bei denen entsprechend dem jeweils aktuellen Stand der Technik in großem Umfang eine neue Technologie eingesetzt wird, sowie für andere Verarbeitungsvorgänge, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, insbesondere dann, wenn diese Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren. Eine Datenschutz-Folgenabschätzung sollte auch durchgeführt werden, wenn die personenbezogenen Daten für das Treffen von Entscheidungen in Bezug auf bestimmte natürliche Personen im Anschluss an eine systematische und eingehende Bewertung persönlicher Aspekte natürlicher Personen auf der Grundlage eines Profiling dieser Daten oder im Anschluss an die Verarbeitung besonderer Kategorien von personenbezogenen Daten, biometrischen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten sowie damit zusammenhängende Sicherungsmaßregeln verarbeitet werden. Gleichermaßen erforderlich ist eine Datenschutz-Folgenabschätzung für die weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen, oder für alle anderen Vorgänge, bei denen nach Auffassung der zuständigen Aufsichtsbehörde die Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, insbesondere weil sie die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern oder weil sie systematisch in großem Umfang erfolgen. Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.[41]

41 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 91.

1.4 Die Aufsichtsbehörden

Die Kompetenzen der Aufsichtsbehörden, die die Privatwirtschaft kontrollieren und beraten, hat der Gesetzgeber in Kapitel IV der DS-GVO festgelegt. Die Einrichtung und Organisation der Aufsichtsbehörden obliegen in Deutschland jedoch den jeweiligen Bundesländern.[42]

Zur Sicherstellung der EU-weiten einheitlichen Auslegung des Datenschutzes nach der DS-GVO wird die Arbeit der Aufsichtsbehörden in einigen Bereichen durch den Europäischen Datenschutzausschuss, einem Gremium, in dem je eine Aufsichtsbehörde eines jeden EU-Mitgliedstaates vertreten ist und das sogenannte Kohärenzverfahren koordiniert.[43]

1.4.1 Zusammenarbeit (Art. 62 DS-GVO)

Neben den Regeln über die federführende Aufsichtsbehörde im One-Stop-Shop-Verfahren (Art. 56, 60)[44], über die Amtshilfe unter Aufsichtsbehörden in der Europäischen Union (Art. 61) und über die internationale Zusammenarbeit (Art. 50) hat der Unionsgesetzgeber in Art. 62 erstmals detaillierte Vorgaben für gemeinsame Maßnahmen der Datenschutzbehörden der Union gemacht.[45]

Die Vorschriften des Art. 61 tritt, neben weitere Regelungen, zur Koordinierung von aufsichtsrechtlichen Maßnahmen zum Schutz personenbezogener Daten. Im Anwendungsbereich der DS-GVO sind die Zusammenarbeit (Art. 60), die Amtshilfe (Art. 61) und die Kohärenz (Art. 63) zu nennen.

Von der Zusammenarbeit und der Kohärenz unterscheiden sich gemeinsame Maßnahmen vor allem dadurch, dass erstere auf Fassung eines gemeinsamen Beschlusses und letztere insbesondere auf die gemeinsame Untersuchung und Durchsetzung gerichtet sind.[46]

---

42 *Gola et al.,* Datenschutz-Grundverordnung im Überblick, 2. Aufl. 2017, S. 65, 5.8.3 Abs. 1.
43 *Gola et al.,* Datenschutz-Grundverordnung im Überblick, 2. Aufl. 2017, S. 65, 5.8.3 Abs. 1.
44 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 56, 60 DSGVO.
45 *Bäcker,* Datenschutz-Grundverordnung, S. 916, Rn. 1, Art. 62 DSGVO.
46 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, S. 912, Rn. 8, Art. 62 DSGVO.

An gemeinsamen Maßnahmen nehmen gem. Art. 62 Abs. 1 Mitglieder und Bedienstete der Aufsichtsbehörden anderer Mitgliedsstaaten teil.[47]

Art. 62 Abs. 2 enthält im Vergleich zu Abs. 1 Sonderregelungen für Fälle grenzüberschreitender Datenverarbeitung. Demnach ist die Aufsichtsbehörde eines Mitgliedstaats berechtigt, an gemeinsamen Maßnahmen teilzunehmen, wenn der Verantwortliche oder der Auftragsverarbeiter im Gebiet ihrer örtlichen Zuständigkeit über eine oder mehrere Niederlassung(en) verfügt oder wenn die Verarbeitungsvorgänge voraussichtlich auf eine bedeutende Zahl betroffener Personen in dem Mitgliedstaat erhebliche Auswirkungen haben.[48]

Die Voraussetzungen für eine Beteiligung der Aufsichtsbehörden an gemeinsamen Maßnahmen knüpfen weitgehend an die Definition der betroffenen Aufsichtsbehörde in Art. 4 Nr. 22[49] an. Nicht in der Teilnahmeberechtigung enthalten ist der Fall des Art. 4 Nr. 22 lit. c. Somit berechtigt der Eingang einer Beschwerde bei der Aufsichtsbehörde nicht zur Teilnahme an gemeinsamen Maßnahmen.[50] Erhöhte Anforderungen stellt Art. 62 Abs. 2 an die Anzahl der von den Auswirkungen der Datenverarbeitung betroffenen Personen. Wohingegen Art. 4 Nr. 22 lit. b keine Aussage zur Anzahl der betroffenen Personen trifft, fordert der Gesetzgeber in Art. 62 Abs. 2 S. 1, dass eine bedeutende Zahl von Personen im Mitgliedstaat von der Datenverarbeitung erheblich betroffen wird. Doch sind in der praktischen Anwendung keine überhöhten Anforderungen an die Bewertung einer bedeutenden Zahl betroffener Personen zu stellen. Die Norm ist unter Berücksichtigung des Primärrechts auszulegen, demzufolge gemäß Art. 197 Abs. 1 AEUV[51] die effektive Durchführung des Unionsrechts durch die Mitgliedstaaten als Frage von gemeinsamem Interesse zu berücksichtigen ist.[52]

---

47 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, Peuker, S. 1045, Rn. 12, Art. 62 DSGVO.

48 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 62997 von 87533, Rn. 15.

49 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 22 DSGVO.

50 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, S. 912, Rn. 7, Art. 62 DSGVO.

51 *Vedder/Heintschel von Heinegg* (Hrsg.), Europäisches Unionsrecht, Vertrag über die Arbeitsweise der Europäischen Union, Art. 197 Abs. 1 AEUV.

52 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, Peuker, S. 1046, Rn. 14, Art. 62 Abs. 2 DSGVO.

Art. 62 Abs. 3 enthält in zweierlei Hinsicht Vorgaben zur exterritorialen Wirkung von Aufsichtsbefugnissen. Zum einen kann die einladende Aufsichtsbehörde nach Art. 62 Abs. 3 S. 1, 1. Alt gemäß dem Recht des eigenen Mitgliedstaats und mit Genehmigung der unterstützenden Aufsichtsbehörde den Mitgliedern oder Bediensteten der unterstützenden Aufsichtsbehörde, die an den gemeinsamen Maßnahmen beteiligt sind, eigene Befugnisse einschließlich Untersuchungsbefugnisse übertragen. Zum anderen kann die einladende Aufsichtsbehörde nach Art. 62 Abs. 3 S. 1, 2. Alt, soweit dies nach ihrem nationalen Recht zulässig ist, den Mitgliedern oder Bediensteten der unterstützenden Aufsichtsbehörde gestatten, ihre fremden Untersuchungsbefugnisse nach dem Recht des Mitgliedstaats der unterstützenden Aufsichtsbehörde auszuüben.[53]

Art. 62 Abs. 4 – 6 enthalten umfangreiche Regelungen zur Haftung der an einer gemeinsamen Maßnahme beteiligten Aufsichtsbehörden im Innen- sowie im Außenverhältnis. Die Regelung ist auf Initiative der im Rat der Europäischen Union vertretenen Mitgliedstaaten in die DS-GVO[54] aufgenommen worden und dient der teilweisen Beschränkung haftungsrechtlicher Risiken.[55] Für die an der gemeinsamen Maßnahme beteiligten Bediensteten haftet der Mitgliedstaat der einladenden Behörde.[56]

Nach der Vorschrift des Art. 62 Abs. 7 sind Aufsichtsbehörden befugt, innerhalb ihres Hoheitsgebiets einstweilige Maßnahmen zu ergreifen, wenn eine Aufsichtsbehörde entgegen Art. 62 Abs. 2 S. 2 innerhalb eines Monats ihrer Pflicht zur Einladung nicht nachkommt. Da der Termin zur Einladung abhängig ist von der Sachverhaltsaufklärung durch die einladende Behörde und sie diesbezüglich einen Ermessensspielraum hat, ist im Einzelfall unklar, zu welchem Zeitpunkt sie zur Einladung verpflichtet ist. Die Frist beginnt z.B. dann, wenn sie nach außen die Absicht bekundet hat, gemeinsame Maßnahmen zu ergreifen.[57]

---

53 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 63100 von 87533, Rn. 21, Art. 62 Abs. 3 DSGVO.

54 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), DSGVO - Datenschutz Grundverordnung.

55 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 63151 von 87533, Rn. 25, Art. 62 Abs. 4 - 6 DSGVO.

56 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, S. 1109, Rn. 10 Satz 1, Art. 62 Abs. 4 - 6 DSGVO.

57 *Bäcker,* Datenschutz-Grundverordnung, S. 921 Abs. 7, Rn. 18 DSGVO.

1.4.2 Kohärenz (Art. 63 DS-GVO)

Art. 63 DS-GVO führt aus: Um zur einheitlichen Anwendung der Verordnung in der gesamten Union beizutragen, arbeiten die Aufsichtsbehörden im Rahmen des in diesem Abschnitt beschriebene Kohärenzverfahrens untereinander und gegebenenfalls mit der Kommission zusammen.[58]

Kohärenz[59] bedeutet begrifflich zum einen Zusammenhang und beschreibt zum anderen im physikalischen Sinn die Eigenschaft von Lichtbündeln, die die gleiche Wellenlänge und Schwingungsart haben. Letzteres beschreibt am ehesten, welches Ziel das Kohärenzverfahren gem. Art. 64 – 66 verfolgt. Das Kohärenzverfahren ist das Bindemittel „Harmonisierung der Rechtsanwendung[60]“, welches den europäischen Verbund zusammenhält und das Tor nach Brüssel ist.[61]

Das Kohärenzverfahren weist strukturell organisiert verschiedene Verfahrenselemente auf, etwa durch die Einbindung des Ausschusses (dazu Art. 68 DS-GVO) oder der Möglichkeit zu einseitigen Dringlichkeitsmaßnahmen durch eine betroffene Aufsichtsbehörde.[62]

Die nachfolgenden Art. 64 (Stellungnahme des Ausschusses), 65 (Streitbeilegung durch den Ausschuss), 66 (Dringlichkeitsverfahren) und 67 (Informationsaustausch) konkretisieren die Durchführung des Kohärenzverfahrens.[63]

Erwägungsgrund 135[64] beschreibt, wie man die einheitliche Anwendung der DS-GVO in der gesamten Union sicherstellen sollte. Er fordert die Einführung eines Verfahrens zur Gewährleistung einer einheitlichen Rechtsanwendung für die Zusammenarbeit zwischen den Aufsichtsbehörden, das sogenannte Kohärenzverfahren. Es soll insbesondere dann angewendet werden, wenn eine Aufsichtsbehörde beabsichtigt, eine Maßnahme zu

---

58 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 63 DSGVO.

59 *DUDEN Onlien,* Kohärenz, https://www.duden.de/rechtschreibung/Kohaerenz.

60 *Voßhoff, Andrea, Hermerschmidt, Sven* PinG - Privacy in Germany Heft 02/2016, 56.

61 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 63476 von 87533, Rn. 11, Art. 63 DSGVO.

62 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, S. 1054, Rn. 4, Art. 63 DSGVO.

63 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, S. 1111, Rn. 2, Art. 64 - 67 DSGVO.

64 Amtsblatt der Europäischen Union 04.05.2016 (Erwägungsgrund 135 Satz 1).

erlassen, die rechtliche Wirkungen in Bezug auf Verarbeitungsvorgänge entfalten soll, die für eine bedeutende Zahl betroffener Personen in mehreren Mitgliedstaaten erhebliche Auswirkungen haben. Ferner sollte es zur Anwendung kommen, wenn eine betroffene Aufsichtsbehörde oder die Kommission beantragt, dass die Angelegenheit im Rahmen des Kohärenzverfahrens behandelt wird. Diese Forderung wurde in Art. 64 umgesetzt.[65]

Erwägungsgrund 135

Um die einheitliche Anwendung dieser Verordnung in der gesamten Union sicherzustellen, sollte ein Verfahren zur Gewährleistung einer einheitlichen Rechtsanwendung (Kohärenzverfahren) für die Zusammenarbeit zwischen den Aufsichtsbehörden eingeführt werden. Dieses Verfahren sollte insbesondere dann angewendet werden, wenn eine Aufsichtsbehörde beabsichtigt, eine Maßnahme zu erlassen, die rechtliche Wirkungen in Bezug auf Verarbeitungsvorgänge entfalten soll, die für eine bedeutende Zahl betroffener Personen in mehreren Mitgliedstaaten erhebliche Auswirkungen haben. Ferner sollte es zur Anwendung kommen, wenn eine betroffene Aufsichtsbehörde oder die Kommission beantragt, dass die Angelegenheit im Rahmen des Kohärenzverfahrens behandelt wird. Dieses Verfahren sollte andere Maßnahmen, die die Kommission möglicherweise in Ausübung ihrer Befugnisse nach den Verträgen trifft, unberührt lassen.[66]

65 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 63729 von 87533, Rn. 2.

66 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Erwägungsgrund 135.

1.5 *Ziel des Datenschutzes*

Erwägungsgrund 1 führt aus, dass der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ein Grundrecht ist. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“)[67] sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.[68]

Nachfolgende Grafik stellt die Umsetzung des Grundrechts auf den Datenschutz dar.[69]

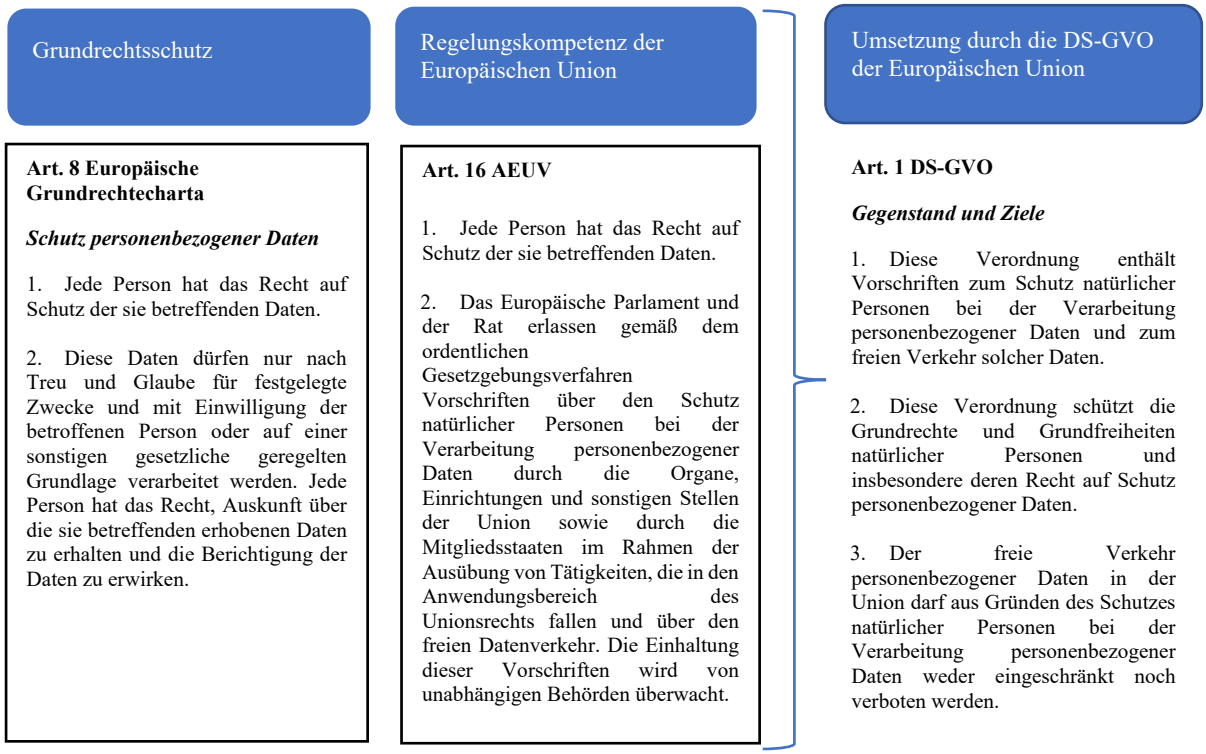

Abbildung 1: Umsetzung des Grundrechts auf Datenschutz[70]

67 *Vedder/Heintschel von Heinegg* (Hrsg.), Europäisches Unionsrecht, Art. 8 GR-Charta.
68 *Vedder/Heintschel von Heinegg* (Hrsg.), Europäisches Unionsrecht, Art. 16 AEUV, S. 345.
69 *Gola et al.,* Datenschutz-Grundverordnung im Überblick, 2. Aufl. 2017.
70 *Gola et al.,* Datenschutz-Grundverordnung im Überblick, 2. Aufl. 2017, S. 23, Abschnitt 4.1.

1.6 Artikel 1 DS-GVO Gegenstand und Ziele

Art. 1 ist die **Leitnorm** der Datenschutz-Grundverordnung: Sie formuliert die generelle Zwecksetzung, nämlich den Schutz der personenbezogenen Daten und den Schutz des freien Datenverkehrs. Gleichzeitig macht Abs. 1 Vorgaben für den Ausgleich zwischen beiden Zielen, wenn es zu einem Konflikt kommen sollte. Die Vorschrift bündelt damit die Kernaussage; sie ist als Interpretationsdirektive zu verstehen. Sie dient als Auslegungshilfe für alle Normen der DS-GVO, insbesondere die vielfältigen unbestimmten Rechtsbegriffe.[71]

Art.1 gehört zu den Normen der DS-GVO, die im Gesetzgebungsverfahren am wenigsten umstritten waren. Schon der erste Kommissionsentwurf enthielt die Formulierung, die letztlich verabschiedet worden ist.[72]

Art. 1 Abs. 1 beschriebt als Zweck des Gesetzes den Schutz des **Einzelnen** vor Beeinträchtigung des Persönlichkeitsrechts. Der Begriff des „Persönlichkeitsrechts“ wurde erstmals 1990 in das BDSG aufgenommen und ist eine Reaktion auf das sog. Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahre 1983. Das Urteil ist ein Meilenstein, denn mit ihm räumte das Bundesverfassungsgericht dem Datenschutz erstmals **Verfassungsrang** ein. Konkret stellt es fest, dass das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz geschützte sog. allgemeine Persönlichkeitsrecht auch ein Recht auf informationelle Selbstbestimmung umfasst.[73]

Die für den Art. 1 erforderliche bzw. genutzte Erwägungsgründe finden sich in den Erwägungsgründen 1 bis 7 wieder. **Erwägungsgrund 1** bestätigt das Grundrecht gemäß Artikel 8 Abs. 1 der Charta der Grundrechte der Europäischen Union sowie Artikel 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV). [74]

---

71 *J. Philipp Albrecht,* Datenschutzrecht, Seite. 241, Rn. 1, Ziele und Funktion der Vorschrift.
72 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Seite. 31, RN 3, Abs.2.
73 *S. Gierschmann,* Systematischer Praxiskommentar Datenschutzrecht (E-Book), 2014, Seite. 4, Rn.10.
74 Amtsblatt der Europäischen Union 04.05.2016.

Der Erwägungsgrund 2 beschreibt die Wahrung der Grundrechte:

„die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Diese Verordnung soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen“ [75]

Erwägungsgrund 3 / Harmonisierung

Dieser beschreibt den Zweck der versuchten Harmonisierung der Datenschutzvorschriften durch die RL 95/46/EG. Der Erwägungsgrund 4 zielt erneut auf die Verarbeitung personenbezogener Daten ab, wie nachfolgend deutlich wird. [76]

Erwägungsgrund 4 / Einklang mit anderen Rechten:

Die Verarbeitung personenbezogener Daten sollte in den Diensten der Menschheit stehen. Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden. Diese Verordnung steht im Einklang mit allen Grundrechten und achtet alle Freiheiten und Grundsätze, die mit der Charta anerkannt wurden und in den Europäischen Verträgen verankert sind, insbesondere Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, Schutz personenbezogener Daten, Gedanken-, Gewissens- und Religionsfreiheit, Freiheit der Meinungsäußerung und Informationsfreiheit, unternehmerische Freiheit, Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren und Vielfalt der Kulturen, Religionen und Sprachen. [77]

75 Amtsblatt der Europäischen Union 04.05.2016.
76 Amtsblatt der Europäischen Union 04.05.2016.
77 Amtsblatt der Europäischen Union 04.05.2016.

Erwägungsgrund 5 / Zusammenarbeit der Mitgliedstaaten zum Datentausch:

Die wirtschaftliche und soziale Integration als Folge eines funktionierenden Binnenmarkts hat zu einem deutlichen Anstieg des grenzüberschreitenden Verkehrs personenbezogener Daten geführt. Der unionsweite Austausch personenbezogener Daten zwischen öffentlichen und privaten Akteuren einschließlich natürlichen Personen, Vereinigungen und Unternehmen hat zugenommen. Das Unionsrecht verpflichtet die Verwaltungen der Mitgliedstaaten, zusammenzuarbeiten und personenbezogene Daten auszutauschen, damit sie ihren Pflichten nachkommen oder für eine Behörde eines anderen Mitgliedstaats Aufgaben durchführen können. [78]

Erwägungsgrund 6 / Gewährleistung eines hohen Datenschutzniveaus trotz Zunahme des Datenaustausches:

Rasche technologische Entwicklungen und die Globalisierung haben den Datenschutz vor neue Herausforderungen gestellt. Das Ausmaß der Erhebung und des Austauschs personenbezogener Daten hat eindrucksvoll zugenommen. Die Technik macht es möglich, dass private Unternehmen und Behörden im Rahmen ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zurückgreifen. Zunehmend machen auch natürliche Personen Informationen öffentlich weltweit zugänglich. Die Technik hat das wirtschaftliche und gesellschaftliche Leben verändert und dürfte den Verkehr personenbezogener Daten innerhalb der Union sowie die Datenübermittlung an Drittländer und internationale Organisationen noch weiter erleichtern, wobei ein hohes Datenschutzniveau zu gewährleisten ist.[79]

Erwägungsgrund 7 / Rechtsrahmen und Vertrauensbasis durch Sicherheit und Kontrolle:

Diese Entwicklungen erfordern einen soliden, kohärenteren und klar durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union, da es von großer Wichtigkeit ist, eine Vertrauensbasis zu schaffen, die die digitale Wirtschaft dringend benötigt, um im Binnenmarkt weiter wachsen zu können. [2]Natürliche Personen sollten die Kontrolle

78 Amtsblatt der Europäischen Union 04.05.2016.

79 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 6.

über ihre eigenen Daten besitzen. [3]Natürliche Personen, Wirtschaft und Staat sollten in rechtlicher und praktischer Hinsicht über mehr Sicherheit verfügen.

Die Erwägungsgründe zum Artikel 1 DS-GVO (1 - 7) zeigen sehr deutlich die Grundlagen des Datenschutzes auf. Dabei wird bereits im **Erwägungsgrund 1** sehr explizit auf den Datenschutz als Grundrecht hingewiesen. Ob als Basis die Charta der Grundrechte oder auch die Arbeitsweise der Europäischen Union.[80]

1.7 Sachlicher Anwendungsbereich (Artikel 2 DS-GVO)

Art. 2 Abs. 1 beschreibt den sachlichen Anwendungsbereich der DS-GVO orientiert an den Zielen, die insbesondere in Art. 1 skizziert werden, aber auch bereits mit der DSRL verfolgt wurden, nämlich den Schutz natürlicher Personen durch Gefährdungen des allgemeinen Persönlichkeitsrechts, die mit der automatisierten Datenverarbeitung oder der Speicherung von Daten in Dateisystemen auf Grundlage manueller Datenverarbeitung einhergehen. Die Erfassung von Vorgängen manueller Datenverarbeitung soll einer Umgehung der Anwendbarkeit des DS-GVO vorbeugen.[81] Die Vorschrift regelt den sachlichen Anwendungsbereich der gesamten DS-GVO. Sie ist damit die Grundlage für die Anwendung aller in Ihren enthaltenen Vorschriften. Sie wählt in Abs. 1 eine sehr breite Grundlage für die Anwendung der Verordnung und macht diese nur von der Verarbeitung personenbezogener Daten abhängig.[82]

Die DS-GVO konkretisiert so die Rechte von Unionsbürgern nach Art. 8 GRCh, wonach jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat. Dabei wird aber nicht jede Art der Datenverarbeitung in Bezug genommen, sondern lediglich die in Abs. 1 genannten. Zugleich verfolgt Art. 2 Abs. 1 das Ziel, den grenzüberschreitenden Verkehr mit personenbezogenen Daten zu harmonisieren und zu regulieren.[83]

---

80 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 7.

81 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, B. Kommentierung, Art. 2, Rn. 17.

82 *J. Philipp Albrecht,* Datenschutzrecht, S. 253, Rn. 1, I. Ziel und Funktion.

83 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, B Kommentierung Art. 2, Rn. 18.

Ausnahmen von der Geltung der Verordnung regelt insbesondere Abs. 2, wonach die Verordnung auf Verarbeitung personenbezogener Daten in den dort genannten Fällen keine Anwendung findet, obgleich die Voraussetzungen des Art. 2 Abs. 1 erfüllt sind.[84] Obwohl jede Verarbeitung personenbezogener Daten nach Abs. 1 eigentlich in den Anwendungsbereich der DS-GVO fällt, lässt Abs. 2 in vier Verarbeitungsbereichen eine Ausnahme gelten.[85]

1.7.1 Fehlender Anwendungsbereich des Unionsrechts (Abs.2 lit. a)

- Art. 2 Abs. 2 und Abs. 3 DS-GVO normieren **Ausnahmen** von der sachlichen Anwendbarkeit der DS-GVO für Bereiche, die spezialgesetzlich geregelt sind, für die der Gesetzgeber keinen Regelungsbedarf gesehen hat oder die nicht in die Regelungskompetenzen der Union fallen.[86] Die Vorschrift korrespondiert mit der begrenzten Rechtsetzungsbefugnis der Union, wie sie sich aus Art. 16 Abs. 2 AEUV ergibt. Nach Art. 16 Abs. 2 AEUV erlassen das Parlament und der Rat Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, sofern diese durch die Organe, Einrichtungen und sonstigen Stellen der Union erfolgt, sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen. Im Umkehrschluss ist diejenige Tätigkeit der Nationalstaaten, die nicht von der Rechtsetzungsbefugnis der Union erfasst ist, zugleich von der Geltung des DS-GVO ausgenommen.[87]

1.7.2 Gemeinsame Außen- und Sicherheitspolitik

- Die zweite Ausnahme betrifft nach Abs. 2 lit. b alle Verarbeitungen personenbezogener Daten, die die Mitgliedstaaten im Rahmen von Tätigkeiten durchführen, die in den Anwendungsbereich von Titel V Kapitel 2 EUV[88] fallen.[89]
- Ausgenommen ist weiter eine Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen des auswärtigen Handelns und der Gemeinsamen

---

84 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, B. Kommentierung, Art.2, Rn. 19.
85 *J. Philipp Albrecht,* Datenschutzrecht, S. 256, Rn. 17.
86 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Seite 55, Rn.14.
87 *Gola et al.,* Datenschutz-Grundverordnung im Überblick, 2. Aufl. 2017, Position 1869 von 87533, Rn. 33.
88 *Vedder/Heintschel von Heinegg* (Hrsg.), Europäisches Unionsrecht, EUV - EU-Vertrag.
89 *J. Philipp Albrecht,* Datenschutzrecht, Seite 257, Rn 22 Abs. 1.

Außen- und Sicherheitspolitik (GASP) gemäß Titel V Kapitel 2 EUV (Art. 23 – 46 EUV). Die Ausnahme liegt darin begründet, dass Art. 39 EUV eine eigene Ermächtigungsgrundlage enthält, aufgrund derer der Rat Vorschriften erlassen kann über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Titel V Kapitel 2 fallen. Insoweit ist zweifelhaft, ob der Datenschutz – jedenfalls nach Erlass derartiger Vorschriften – unmittelbar an Art. 7 und 8 GRCh zu messen ist.[90]

1.7.3 Persönliche oder familiäre Tätigkeiten

- Der Ausnahmetatbestand des Art. 2 Abs. 2 lit. c, die sog. „Haushaltsausnahme" oder auch das Haushaltsprivileg, war bereits Bestandteil des Art. 3 Abs. 2 2. Spiegelstrich der DSRL und des BDSG a.F. Die Regelung folgt dem Gedanken, dass die häusliche Privatsphäre ihrerseits den grundrechtlichen Schutz des allgemeinen Persönlichkeitsrechts genießt und so von der staatlichen Regelungsbefugnis ausgenommen sein soll.
- Erwägungsgrund 18 enthält nur ansatzweise Hinweise auf den Umfang der Regelung. So soll „**auch das Führen**" eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten" Ausdruck persönlicher oder familiärer Datenverarbeitungstätigkeiten sein können. Insbesondere Art. 4 enthält insoweit keine Definitionen der Begriffe „**persönlich**" und „**familiär**". Sprachlich ist eine Abweichung festzustellen zum Wortlaut etwa der englischen und der französischen Fassung, die anstelle des Begriffs „**private**" in der deutschen Fassung die Begriffe „**household**" bzw. „**domestique**" verwenden. Die genannten Fassungen dürften somit den Regelungsgehalt besser zum Ausdruck bringen, weil sie stärker als die deutsche Fassung auf die häusliche Privatsphäre abstellen.[91]

90 *Gola et al.,* Datenschutz-Grundverordnung im Überblick, 2. Aufl. 2017, Rn. 36.
91 *Gola et al.,* Datenschutz-Grundverordnung im Überblick, 2. Aufl. 2017, Rn. 37 - 38.

Erwägungsgrund 18

Diese Verordnung gilt nicht für die Verarbeitung von personenbezogenen Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird. Als persönliche oder familiäre Tätigkeiten könnte auch das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten gelten. Diese Verordnung gilt jedoch für die Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen.[92]

1.7.4 Straftatenbekämpfung und Gefahrenabwehr

- Die vierte Ausnahme gilt nach Abs. 2 lit. d für alle Verarbeitungen personenbezogener Daten, die die zuständigen Behörden „zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“, vornehmen.[93]
- Erwägungsgrund19 führt ergänzend an, dass nur die in lit. d genannten Tätigkeiten von der Privilegierung erfasst sind; andere Aufgaben, die den für repressives oder präventives Handeln zuständigen Behörden übertragen sind oder werden, unterfallen weiterhin der Geltung der DS-GVO. Zugleich ist auch das Handeln unzuständiger Behörden auf dem Tätigkeitsfeld nach lit. d weiterhin der DS-GVO unterworfen. Dies gilt gleichermaßen für das Tätigwerden nichtöffentlicher Stellen auf dem Gebiet der Strafverfolgung.[94]

Erwägungsgrund 19

Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor

92 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 18.
93 *J. Philipp Albrecht,* Datenschutzrecht, S. 261, Rn. 37.
94 *Gola et al.,* Datenschutz-Grundverordnung im Überblick, 2. Aufl. 2017, Position 1961, Rn. 47.

und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie der freie Verkehr dieser Daten sind in einem eigenen Unionsrechtsakt geregelt. Deshalb sollte diese Verordnung auf Verarbeitungstätigkeiten dieser Art keine Anwendung finden. Personenbezogene Daten, die von Behörden nach dieser Verordnung verarbeitet werden, sollten jedoch, wenn sie zu den vorstehenden Zwecken verwendet werden, einem spezifischeren Unionsrechtsakt, nämlich der Richtlinie (EU) 2016 / 680 des Europäischen Parlaments und des Rates unterliegen. Die Mitgliedstaaten können die zuständigen Behörden im Sinne der Richtlinie (EU) 2016 / 680 mit Aufgaben betrauen, die nicht zwangsläufig für die Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, ausgeführt werden, so dass die Verarbeitung von personenbezogenen Daten für diese anderen Zwecke insoweit in den Anwendungsbereich dieser Verordnung fällt, als sie in den Anwendungsbereich des Unionsrechts fällt. In Bezug auf die Verarbeitung personenbezogener Daten durch diese Behörden für Zwecke, die in den Anwendungsbereich dieser Verordnung fallen, sollten die Mitgliedstaaten spezifischere Bestimmungen beibehalten oder einführen können, um die Anwendung der Vorschriften dieser Verordnung anzupassen. In den betreffenden Bestimmungen können die Auflagen für die Verarbeitung personenbezogener Daten durch diese zuständigen Behörden für jene anderen Zwecke präziser festgelegt werden, wobei der verfassungsmäßigen, organisatorischen und administrativen Struktur des betreffenden Mitgliedstaats Rechnung zu tragen ist. Soweit diese Verordnung für die Verarbeitung personenbezogener Daten durch private Stellen gilt, sollte sie vorsehen, dass die Mitgliedstaaten einige Pflichten und Rechte unter bestimmten Voraussetzungen mittels Rechtsvorschriften beschränken können, wenn diese Beschränkung in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz bestimmter wichtiger Interessen darstellt, wozu auch die öffentliche Sicherheit und die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder die Strafvollstreckung zählen, einschließlich des Schutzes vor und der Abwehr von Gefahren

für die öffentliche Sicherheit. Dies ist beispielsweise im Rahmen der Bekämpfung der Geldwäsche oder der Arbeit kriminaltechnischer Labors von Bedeutung.[95]

Abs. 3 regelt die fortgesetzte Anwendbarkeit der Verordnung (EG) Nr. 45/ 2001 auf die Tätigkeit der Unionsorgane und ihrer Untergliederungen, zugleich die Anwendbarkeit weiterer Rechtsakte, die die Datenverarbeitung durch die Unionsorgane zum Gegenstand haben; zugleich wird vorgeschrieben, dass die betreffenden Rechtsakte an die Regelungen der DS-GVO anzupassen sind.[96]

Schließlich bestimmt Abs. 4 die Fortgeltung der E-Commerce-Richtlinie 2000/ 31/ EG bezogen auf die Verantwortlichkeit von Vermittlern.[97]

Artikel 2 nimmt die **Erwägungsgründe** 14 bis 21 in Bezug. Hier sind weiterführende Informationen einzuholen.[98]

95 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 19.

96 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, B. Kommentierung, Art.2, Rn. 20.

97 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, B. Kommentierung, Art.2, Rn. 21.

98 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgründe 14 - 21.

1.8 Räumlicher Geltungsbereich (Artikel 3 DS-GVO)

1.) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.

2.) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

   a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;
   b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

3.) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines [99]

Art.3 nimmt die **Erwägungsgründe** 22 – 25 in Bezug.

Erwägungsgrund 22 geht davon aus, dass jede Datenverarbeitung im Rahmen der Tätigkeit einer Niederlassung von Datenverarbeitern in der Union, ob als Verantwortliche oder als Auftragsverarbeiter, der Geltung des DS-GVO unterliegen soll, ungeachtet des Ortes der eigentlichen Datenverarbeitung. Zugleich formuliert Erwägungsgrund 22

99 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Artikel 3, Räumlicher Geltungsbereich.

Anforderungen an die Niederlassung als „feste Einrichtung“, ungeachtet der gewählten Organisationsform.[100] [101]

Erwägungsgrund 23 geht von der Notwendigkeit aus, dass eine Datenverarbeitung, die durch einen nicht in der EU niedergelassenen Verantwortlichen oder Auftragsverarbeiter erfolgt, jedenfalls dann der DS-GVO unterfallen soll, wenn die Verarbeitung dazu dient, den betroffenen Personen gegen Entgelt oder unentgeltlich Waren oder Dienstleistungen anzubieten. Ein entsprechendes Anbieten ist dann gegeben, wenn der Datenverarbeiter dies offensichtlich beabsichtigt. Dies soll etwa bei Vertrieb über Websites anzunehmen sein, wenn die Seite eine in der EU gebräuchliche Sprache oder Währung vorgibt, und die Möglichkeit zum Warenerwerb bietet. Dies soll auch gelten, wenn der Verantwortliche Kunden oder Nutzer erwähnt, die in der Union ansässig sind.[102] [103]

Erwägungsgrund 24 sieht die Anwendbarkeit der DS-GVO insbesondere dann als geboten, wenn der Verantwortliche oder der Auftragsverarbeiter das Verhalten einer Person beobachtet und dieses Verhalten innerhalb der Union erfolgt. Dies soll immer dann der Fall sein, wenn Internetaktivitäten nachvollzogen oder Techniken angewendet werden, die die Profilerstellung bezüglich einer Person ermöglichen.[104] *[105]*

---

100 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 2451, Rn. 2.

101 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 22.

102 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 2451, Rn. 2.3

103 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 23.

104 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 2451, Rn. 2.

105 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 24.

Erwägungsgrund 25:

Erwägungsgrund 25 will sicherstellen, dass die DS-GVO auch auf solche Datenverarbeitungen Anwendung findet, die außerhalb der EU stattfinden, die aufgrund Völkerrechts aber dem Recht eines Mitgliedstaates unterfallen, so etwa im Bereich diplomatischer oder konsularischer Vertretungen.[106]

1.8.1 Übermittlung von Daten an Drittländer

Innerhalb des **E**uropäischen **W**irtschafts**r**aumes (**EWR**) dürfen Daten übermittelt werden, wenn die datenschutzrechtlichen Grundsätze und die Bedingungen für die Rechtmäßigkeit der Datenverarbeitung erfüllt werden. Der Datentransfer innerhalb des EWR ist somit dem innerstaatlichen Transfer gleichgestellt. Im Gegenzug dazu müssen bei Übermittlungen in Drittländer, die kein vergleichbares **Datenschutzniveau** gewährleisten, zusätzliche Zulässigkeitsvoraussetzungen erfüllt werden.[107]

Jede Übermittlung personenbezogener Daten, die bereits verarbeitet wurden oder nach ihrer Übermittlung verarbeitet werden sollen, ist nur zulässig, wenn die Bestimmungen der DS-GVO zum Schutze der Rechte von betroffenen Personen vom Verantwortlichen und / oder Auftragsverarbeiter eingehalten werden.[108] (vgl. Erwägungsgrund 101)

Erwägungsgrund 101

Der Fluss personenbezogener Daten aus Drittländern und internationalen Organisationen und in Drittländer und internationale Organisationen ist für die Ausweitung des internationalen Handels und der internationalen Zusammenarbeit notwendig. Durch die Zunahme dieser Datenströme sind neue Herausforderungen und Anforderungen in Bezug auf den Schutz personenbezogener Daten entstanden. Das durch diese Verordnung unionsweit gewährleistete Schutzniveau für natürliche Personen sollte jedoch bei der Übermittlung personenbezogener Daten aus der Union an Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern oder an internationale Organisationen nicht untergraben werden, und zwar auch dann nicht, wenn aus einem Drittland oder von einer internationalen Organisation personenbezogene Daten an

106 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 2451, Rn. 2.
107 *Marzi/Pallwein-Prettner,* Datenschutzrecht, 2018, S. 119, Abschnitt 11, Abs. 1.
108 *Marzi/Pallwein-Prettner,* Datenschutzrecht, 2018, S. 119, Abschnitt 11.1.

Verantwortliche oder Auftragsverarbeiter in demselben oder einem anderen Drittland oder an dieselbe oder eine andere internationale Organisation weiterübermittelt werden. In jedem Fall sind derartige Datenübermittlungen an Drittländer und internationale Organisationen nur unter strikter Einhaltung dieser Verordnung zulässig. Eine Datenübermittlung könnte nur stattfinden, wenn die in dieser Verordnung festgelegten Bedingungen zur Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen vorbehaltlich der übrigen Bestimmungen dieser Verordnung von dem Verantwortlichen oder dem Auftragsverarbeiter erfüllt werden.[109]

Datenexporte in Drittländer bedürfen grundsätzlich geeigneter Garantien, damit das durch die Grundverordnung geschaffene Schutzniveau durch den Datenexport nicht untergraben wird (vgl. Art. 44 DS-GVO). Ein Zertifizierungsmechanismus, zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder Auftragsverarbeiters im Drittland, kann eine solche „geeignete Garantie“ darstellen (vgl. Art. 46 Abs. 2 lit. f), wobei die Datenschutz-Grundverordnung deren Ausgestaltung nicht näher spezifiziert. Im Fokus stehen die Grundrechte und -freiheiten der Betroffenen (vgl. ErwG 2) und diesbezügliche Schutzmechanismen. Die Ausgestaltung geeigneter Garantien für die Datenübermittlung in ein Drittland wurden bereits im Jahr 1998 durch die Art. 29-Datenschutzgruppe auf Basis der DSRL 95/ 46/ EG formuliert[110], wobei eine Anpassung des Papiers an die Datenschutz-Grundverordnung zu erwarten ist. Das Urteil des EuGH zu Safe Harbor stellt dabei aktuell hohe grundrechtliche Anforderungen an den Drittlandexport auf.[111]

109 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).

110 *Datenschutzgruppe 29,* WP 29 - Übermittlung personenbezogener Daten an Drittländer.

111 Große Kammer, Urteil v. 6.10.2015, C-362 / 14 – Safe Harbor Abkommen.

1.8.2 Safe Harbor / EU - US Privacy Shield

Mit Entscheidung vom 26. Juli 2000 gestattete die Europäische Kommission Datenübermittlungen an Unternehmen, die am sog. Safe-Harbor-Programm teilnahmen und die infolgedessen so behandelt werden dürfen, als seien sie in der EU ansässig.[112] Bereits früh wurde Kritik an der unzureichenden Sanktionierung von Verstößen durch die US **F**ederal **T**rade **C**ommission (**FTC**) geübt. Die Europäische Kommission hat in mehreren Entscheidungen Grundsätze des Safe Harbor Abkommens zum Datentransfer in die USA (2000) und Standardvertragsklauseln zum Datentransfer auch in andere Drittstaaten (2004 und 2010) festgelegt. Die Beachtung dieser Vorgaben soll gewährleisten, dass personenbezogene Daten, die in die USA oder andere Drittstaaten übermittelt werden, dort einem angemessenen Datenschutzniveau unterliegen. Allerdings hat die Kommission stets betont, dass die nationalen Aufsichtsbehörden die Datenübermittlung aussetzen können, wenn eine "hohe Wahrscheinlichkeit" besteht, dass die Safe-Harbor-Grundsätze oder Standardvertragsklauseln verletzt werden.[113]

Im Urteil des Europäischen Gerichtshofes (EuGH) erklärte der EuGH am 6.10.2015, dass nationale Datenschutzbehörden unabhängig das angemessene Datenschutzniveau eines Drittstaates prüfen können, womit er die Safe-Harbor Entscheidung (2000/520) für ungültig erklärte. Maßgeblich hierfür war einerseits, dass die Kommission nicht festgestellt hatte, ob die USA tatsächlich ein angemessenes Datenschutzniveau gewährleistet. Ein ausreichender Schutz sei bei dem gewählten System der Selbstzertifizierung nur gewährleistet, wenn wirksame Überwachungs- und Kontrollmechanismen für die Einhaltung der Grundsätze beständen.[114]

Nach Aufhebung der Safe-Harbor-Entscheidung der Europäischen Kommission 2000/520/EG durch den EuGH im sogenannten Schrems-Urteil (Rechtssache C-362/14) steht seit der Entscheidung der Europäischen Kommission (2016 / 1250) vom 12. Juli

112 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, Schröder, S. 762, Rn. 36 zu Art. 45 DS-GVO.

113 *Die Landesbeauftragte für Datenschutz - Bremen,* Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten, https://www.datenschutz.bremen.de/sixcms/detail.php?gsid=bremen236.c.9283.de.

114 Große Kammer, Urteil v. 6.10.2015, C-362 / 14 – Safe Harbor Abkommen.

2016 mit dem „EU – US Privacy Shield“ eine Rechtsgrundlage für Datenübermittlungen in die USA in Form eines Angemessenheitsbeschlusses zur Verfügung.[115]

*Unter einem „**Angemessenheitsbeschluss**“ ist ein Beschluss, der von der Europäischen Kommission gemäß Artikel 45 DS-GVO angenommen wird und durch den festgelegt wird, dass ein Drittland (d. h. ein Land, das **nicht** an die DS-GVO gebunden ist) oder eine internationale Organisation ein angemessenes Schutzniveau für personenbezogene Daten bietet. Im Rahmen dieses Beschlusses werden die innerstaatlichen Rechtsvorschriften des Landes, seine Aufsichtsbehörden und die von ihm eingegangenen internationalen Verpflichtungen berücksichtigt.*[116]

Zu den wesentlichen datenschutzrechtlichen Auflagen im Privacy Shield zählen unter anderem die eigens vorgesehene Beschwerdemöglichkeit von Betroffenen und ein jährlicher Überprüfungsprozess, durch den die Einhaltung der Vorschriften durch die zertifizierten Unternehmen sichergestellt werden soll. Neu eingeführt wurde auch die Verpflichtung von zertifizierten Unternehmen, personenbezogene Daten aus der EU nur so lange speichern, wie sie für ihren ursprünglichen Zweck benötigt werden.[117]

115 *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,* EU-US Privacy Shield und Datenübermittlungen in die USA, https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/EU-US_PrivacyShield_Daten%C3%BCbermittlungenUSA.html.

116 *DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE,* Angemessenheitsbeschluss, https://edps.europa.eu/data-protection/data-protection/glossary_de.

117 *Marzi/Pallwein-Prettner,* Datenschutzrecht, 2018, S. 122.

2 Begriffsbestimmungen

Art. 4 legt die Bedeutung und Reichweite der wesentlichen Begriffe des europäischen Datenschutzrechts fest. Die Norm ist nicht abschließend. Daneben finden sich in Art. 51 („Aufsichtsbehörde“) und Art. 68 („Ausschuss“) sowie in Art. 5 bei der Festlegung der fundamentalen Grundsätze für die Verarbeitung personenbezogener Daten (z.B. „Rechtmäßigkeit“, „Zweckbindung“, „Transparenz“, „Verhältnismäßigkeit“ und „Rechenschaft“) sowie in Art. 9 hinsichtlich besonderer Kategorien personenbezogener Daten erklärende Umschreibungen mit definierendem Charakter. Der Begriff „Kind“ wird weder in Art. 8 selbst noch in Art. 4 definiert. Für die Anwendung des Art. 8 bedarf es aber wegen der geregelten Altersgrenze keiner genaueren Definition. Diese leitet sich gemäß Art. 8 Abs. 3 aus dem Recht der Mitgliedstaaten ab.[118]

Art. 4 DS-GVO enthält Legaldefinitionen für insgesamt 26 verschiedene, in der DS-GVO verwendete Begriffe. Dies stellt eine erhebliche Erweiterung gegenüber der EG-DSRI dar, die in Art. 2 EG-DSRI nur acht Legaldefinitionen enthielt. Diese acht Begriffe werden, teilweise in leicht geänderter Form, auch in der DS-GVO definiert.[119]

2.1 Art. 4 Nr. 1 DS-GVO Personenbezogene Daten (Datum)

Der Begriff des personenbezogenen Datums ist das zentrale Tatbestandsmerkmal der DS-GVO. Auf sekundärrechtlicher Ebene löste dessen Vorhandensein die Anwendung des Datenschutzrechts aus und eröffnet damit den materiellen Anwendungsbereich der DS-GVO. Er stellt die Verknüpfung zwischen der technischen Datenverarbeitung des primär- und verfassungsrechtlichen Schutzes personenbezogener Daten und des Rechts auf informelle Selbstbestimmung i.S.d Art. 7 und 8 GRCh[120] sowie Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

118 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, 3177 von 87533, Rn. 2.
119 *J. Philipp Albrecht,* Datenschutzrecht, Seite 87, Rn.1 Abs.1.
120 *Vedder/Heintschel von Heinegg* (Hrsg.), Europäisches Unionsrecht, GRCh - Grundrechte Charta.

Der Anwendungsbereich der DS-GVO ist nur eröffnet, wenn personenbezogene Daten im Sinne von Art. 4 Nr. 1 verarbeitet werden. Damit kommt dem Begriff des personenbezogenen Datums eine Schlüsselrolle zu.[121] Artikel 4 DS-GVO führt zum Begriff, personenbezogene Daten, folgendes aus. *Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt insbesondere mittels Zuordnung zu einer Kennung wie einem Namen zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann*.[122]

Die Norm definiert das „personenbezogene Datum". Diese Definition ist zentral für den gesamten europäischen Datenschutz, weil das „personenbezogene Datum" den sachlichen Anwendungsbereich der DS-GVO festlegt. Die Vorschrift stellt auf einen Personenbezug ab und verlangt dafür die Identifizierung bzw. Identifizierbarkeit einer natürlichen Person. Allerdings klärt die Vorschrift nicht eindeutig, ob es für die Identifizierbarkeit lediglich auf die Kenntnisnahme Möglichkeiten des jeweiligen Daten Verarbeiters (relativer Ansatz) ankommt oder auch auf die Kenntnisnahme Möglichkeiten Dritter (absoluter Ansatz). Dass ein ausufernder Schutz abzulehnen ist, folgt bereits aus Art. 1 Abs. 2 und dem dazugehörigen **Erwägungsgrund 4**. Demnach dient die DS-GVO nicht nur dem Recht auf Schutz personenbezogener Daten, sondern auch dem Schutz konkurrierender Grundrechte und Grundfreiheiten. [123]

2.1.1 Natürliche Person

Jeder lebende Mensch ist eine natürliche Person. Verstorbene Zählen hierzu nicht, da für sie der Grundsatz der freien Entfaltung der Persönlichkeit, auf dem die DS-GVO fußt, nicht gilt[124], die auch den noch nicht geborenen und den Verstorbenen in den Schutz

121 *Kühling/Klar/Sackmann,* Datenschutzrecht, 4. Aufl. 2018, S.125, Allgemeines Rn. 1.
122 *Kühling/Klar/Sackmann,* Datenschutzrecht, 4. Aufl. 2018, S. 124, Art.4 Nr.1 DSGVO.
123 *Assion,* Kommentar Datenschutz-Grundverordnung, S.55 - 56, Rn.1.
124 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Art. 1, Rn. 12 DSGVO.

miteinbeziehen; siehe jedoch auch § 4 Abs. 1 BlnDSG[125], der Daten verstorbenen einbezieht, soweit **schutzwürdige Belange des Verstorbenen** beeinträchtigt werden können).[126]

Art. 4 Nr. 1 umfasst ohne Einschränkungen „alle Informationen", die sich auf eine Person beziehen und ist daher grundsätzlich weit zu verstehen.[127]

Nach Art. 4 Nr. 1 sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, „personenbezogene Daten". Nach Art. 2 lit. a DSRL sind personenbezogene Daten „**alle Informationen** über eine bestimmte oder bestimmbare natürliche Person". Folglich wurden die Begriffe „bestimmt" und „bestimmbar" lediglich durch „identifiziert" und „identifizierbar" ersetzt. Nach Erwägungsgrund 26 zu Art. 2 lit. a DSRL[128] sollten zur „Bestimmbarkeit alle Mittel berücksichtigt werden, die vernünftigerweise entweder von einem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen". Erwägungsgrund 26 S. 3 zur DS-GVO spricht nunmehr davon, dass „zur Identifizierbarkeit alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden". Inhaltlich ergeben sich aus der neuen Formulierung keine abweichenden Erkenntnisse, weil sie ebenfalls nur auf eine Wahrscheinlichkeitsprognose abstellt.[129]

Auch § 1 Abs. 1 und 2 BDSG a.F.[130] sprachen im Rahmen von personenbezogenen Daten von „Einzelangaben über eine bestimmte oder bestimmbare natürliche Person". Insoweit steht Art. 4 Nr. 1 in der bisherigen Datenschutz-Tradition und bringt im Vergleich zur bisherigen Rechtslage unter der DSRL und dem BDSG als Vorgängerregelungen keine grundlegenden Neuerungen hinsichtlich der Reichweite des Personenbezugs.[131] [132]

---

125 Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz - BlnDSG) Vom 13. Juni 2018 *), BlnDSG - Berliner Datenschutzgesetz.
126 *Erich-Schmidt-Verlag,* Datenschutz-Grundverordnung (DS-GVO), Bundesdatenschutzgesetz (BDSG), 2017, 0200 Art. 4, S. 8, Rn. 4 Abs. 3 DSGVO.
127 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, S.126, Rn. 8.
128 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates.
129 *Bäcker,* Datenschutz-Grundverordnung, S. 125, Rn. 2, Art. 4 Nr. 1 DSGVO (Allgemeines).
130 *Körffer et al.,* Bundesdatenschutzgesetz, 10. Aufl. 2010, § 1 Abs. 1 und 2 BDSG a.F.
131 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 3242 von 87533, Rn. 9.
132 *Assion,* Kommentar Datenschutz-Grundverordnung, S. 56, Rn. 3 f. Art. 4 Nr. 1 DSGVO.

Erwägungsgrund 26

Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Die *Grundsätze* des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.[133]

2.1.2 Betroffene Person

Personenbezogene Daten sind nur solche Informationen, die sich auf eine bestimmte oder bestimmbare bzw. identifizierte oder identifizierbare natürliche Person beziehen. Die DS-GVO bezeichnet diese Person „betroffene Person“ und unterstellt diese durch die Betroffenenrechte einem besonderen Schutz. Im Umkehrschluss folgt daraus, dass nicht-personenbezogene Daten, also anonyme Daten nicht unter die DS-GVO fallen, wohl aber pseudonymisierte Daten, die bei Aufhebung der Pseudonymisierung zu einer Identifizierbarkeit führen. Der Schutz anonymer Daten kann aber aus anderen

133 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 26.

Rechtsvorschriften folgen. Wenngleich es sich bei der DS-GVO um eine Regelung des europäischen Datenschutzrechts handelt, fallen auch Nicht-EU-Bürger unter diese Begriffsdefinition, sofern ihre Daten im Geltungsbereich von Art. 3 verarbeitet werden.[134] Diesem folgt ebenfalls **Erwägungsgrund 14.**

Erwägungsgrund 14

Der durch diese Verordnung gewährte Schutz sollte für die Verarbeitung der personenbezogenen Daten natürlicher Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gelten. Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person.[135]

2.1.3 Natürliche versus juristische Personen

Juristische Personen, Personenmehrheiten und -gruppen sind aus dem Schutzbereich ausgenommen. Soweit Informationen über die Personengruppe aber auf ein identifiziertes oder identifizierbares Mitglied ermöglichen, handelt es sich bei der Information um ein personenbezogenes Datum.[136]

2.1.4 Verstorbene

Aus **Erwägungsgrund 27** S. 1 folgt, dass die DS-GVO nicht für die personenbezogenen Daten Verstorbener gilt. Insofern gibt es keinen „**postmortalen Datenschutz**“[137]. Gleichwohl bestimmt **Erwägungsgrund 27** S. 2, dass die Mitgliedstaaten Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen können. Darüber hinaus darf nicht außer Acht gelassen werden, dass auch Daten eines Verstorbenen womöglich einen Bezug zu einer lebenden Person haben und damit einen Personenbezug aufweisen[138] können, wie etwa Angaben zum Vermögen des Erblassers

134 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, Seite 125, Rn.3, Betroffene Person.
135 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 26.
136 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, Seite 125, Rn.4, Natürliche versus juristische Personen.
137 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Begriff aus Art. 4 Nr. 1, Rn. 9 DSGVO.
138 *Datenschutzgruppe 29,* Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, Stellungnahme 04/2017 zum Begriff "personenbezogener Daten" WP 136, S. 26.

oder Informationen hinsichtlich vererblicher Krankheiten des Verstorbenen.[139] Allerdings hat der BGH in seinem Urteil aus 2018[140] ausgeführt, dass mit dem Tod eines Kontoinhabers eines Sozialen Netzwerkes (in diesem Fall Facebook) der Nutzungsvertrag auf dessen Erblasser übergeht.

Erwägungsgrund 27

Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener. Die Mitgliedstaaten können Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen.[141]

2.1.5 Ungeborenes Leben

Die Frage, ob auch das ungeborene Leben bzw. auch Daten, die sich auf ein noch ungeborenes Kind beziehen, einen Personenbezug im Sinne der DS-GVO aufweisen, wird durch die Verordnung selbst nicht unmittelbar beantwortet. Die Art. 29-Datenschutzgruppe lässt diese Frage offen[142]. Da aber im Fokus der DS-GVO insbesondere die Betroffenenrechte stehen, deren Ausübung nur durch einen bereits lebenden im Sinne von geborenen Menschen erfolgen kann, liegt – unabhängig von der Frage der fehlenden Rechtssubjektivität – die Annahme nahe, dass Daten ungeborener Kinder noch keinen Personenbezug aufweisen.[143]

2.1.6 Information

Ausweislich des Normtextes des Art. 4 Nr. 1 umfasst der Begriff der personenbezogenen Daten auf den ersten Blick „alle Informationen“. Voraussetzung ist dabei, dass diese Informationen Personenbezug aufweisen. Insoweit ist der Begriff grundsätzlich weit zu verstehen und erfasst sowohl persönliche Informationen wie etwa den Namen oder die Anschrift als auch äußere Merkmale wie Geschlecht, Größe oder Gewicht. Darüber

---

139 *Bäcker,* Datenschutz-Grundverordnung, S. 126, Rn. 5, (vgl. KG Berlin Urt. v. 31.5.2017–21 U 9 / 16).

140 BGH - Bundesgerichtshof, 12. Juli 2018 – III ZR 183/17 Bundesgerichtshof - Entscheidungen (2018).

141 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 27.

142 *Datenschutzgruppe 29,* Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, WP 136 zu "personenbezogenen Daten".

143 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, S. 260, Rn. 12.

hinaus zählen hierzu auch weitere Informationen wie etwa Meinungen, Vermögensverhältnisse oder bestehende vertragliche Beziehungen.[144]

Unerheblich sind demgegenüber in welcher Form die Informationen verkörpert oder ausgestaltet sind. Sie können in jedem Format oder auf jedem Datenträger verkörpert und auf beliebigen Datenträgern gespeichert und abrufbar sein.[145]

Unklar ist, ob die Information eine persönlichkeitsrechtliche Implikation aufweisen muss, also ob der Datenschutz ausschließlich an das personenbezogene Datum anknüpft oder auch andere Schutzgüter wie das Persönlichkeitsrecht maßgeblich sind. In diesem Zusammenhang betonen manche[146], dass eine Entpersonalisierung des Datenschutzes drohe, wenn dieser ausschließlich an das Datum als solches anknüpfe, während andere mit Blick auf die Rechtsprechung des BVerfG davon ausgehen, dass es im Rahmen einer automatisierten Datenverarbeitung grundsätzlich kein „unerhebliches", weil nicht personenbezogenes Datum geben könne.[147]

2.1.7 Personenbezug der Information

Der Wortlaut des Art. 4 Nr. 1[148] besagt, dass sich die Information auf eine natürliche Person beziehen muss. Der Personenbezug macht die Person somit zur „betroffenen" Person und eröffnet ihr die Betroffenenrechte der DS-GVO.[149] Aus dem Wortlaut der Verordnung ergibt sich darüber hinaus zum einen, dass der Personenbezug ein eigenständiges Tatbestandsmerkmal darstellt, das unabhängig von einer Identifizierung bzw. Identifizierbarkeit zu prüfen ist, sowie zum anderen, dass ein nicht-personenbezogenes Datum nicht dem Anwendungsbereich der DS-GVO unterfällt.[150]

---

144 *Bäcker,* Datenschutz-Grundverordnung, S. 126, Rn. 8.
145 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, S. 73, Rn. 7, Art. 4 Nr. 1 DSGVO.
146 *Assion,* Kommentar Datenschutz-Grundverordnung, Buchholtz/Stenzel, S. 56, Rn. 2 (Art. 4 Nr. 1 DSGVO).
147 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 3341, Rn. 16.
148 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).
149 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), DSGVO - Datenschutz Grundverordnung.
150 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, S. 260, Rn. 9.

Keinen Personenbezug weisen demzufolge Sachdaten auf, wie z.B. die Aussage „Der Kölner Dom ist rund 157 Meter hoch“. Andererseits ist stets zu beachten, dass auch bei Sachdaten ein Personenbezug angelegt sein kann. Dies ist beispielsweise bei Anruflisten der Fall, weil diese Daten (Telefonnummer, Anrufzeit) Informationen über die beteiligten Personen, wie etwa deren Privatleben, soziale Beziehungen oder unter Umständen sogar den Wohnort, enthalten[151]. Grundsätzlich muss die Abgrenzung zwischen einem Sachdatum und einem personenbezogenen Datum einem kontextbezogenen Ansatz folgen. So hat die Art. 29-Datenschutzgruppe[152] festgestellt, dass ein personenbezogenes Datum dann vorliegen kann, wenn in dem Datum ein „Inhaltselement“ („dann vorhanden, wenn (…) Informationen über eine bestimmte Person gegeben werden, und zwar unabhängig vom Zweck aufseiten des für die Verarbeitung Verantwortlichen oder eines Dritten oder von den Auswirkungen dieser Information auf die betroffene Person“), ein Zweckelement gegeben, wenn die Daten unter Berücksichtigung aller Begleitumstände mit dem Zweck verwendet werden bzw. verwendet werden könnten, eine Person zu beurteilen, in einer bestimmten Weise zu behandeln oder ihre Stellung oder ihr Verhalten zu beeinflussen“) oder ein „Ergebniselement“ (dann gegeben, wenn „ihre Verwendung unter Berücksichtigung aller jeweiligen Begleitumstände auf die Rechte und Interessen einer bestimmten Person auswirken könnte“) vorhanden ist[153]. Grenzfälle ergeben sich in datenschutzrechtlicher Hinsicht insbesondere bei Wearables (Technologie, die am Körper und / oder am Kopf getragen werden können), wo tragbare und an das Internet angeschlossene Computersysteme Daten, wie Laufwege einer Person, generieren. Insofern ist stets eingehend zu prüfen, ob einem Datum ein Personenbezug innewohnt. Faktisch wird es im Ergebnis nur wenige Daten geben, die sich einer Auswertung mit Blick auf den Personenbezug entziehen. Auch der durch einen Regensensor ohne menschliches Zutun in Gang gesetzte Scheibenwischer eines Fahrzeugs lässt zwischenzeitlich Rückschlüsse über die vom Fahrer bestimmte Fahrstrecke zu.[154]

---

151 *Datenschutzgruppe 29,* Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, WP 136, S. 13.

152 *Datenschutzgruppe 29*, Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, DSGVO angenommen am 3. Oktober 2017.

153 *Datenschutzgruppe 29,* Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, WP 136, S. 11 f.

154 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 3242 von 87533, Rn. 9.

2.1.8 Identifizierte oder identifizierbare Person

Die Information muss sich nach Art. 4 Nr. 1 auf eine „identifizierte oder identifizierbare" Person beziehen. Für die rechtliche Beurteilung ist es im Rahmen von Art. 4 Nr. 1 ohne Belang, unter welchen Begriff sich ein Tatbestand subsumieren lässt. Während die DS-GVO den Begriff der identifizierbaren Person ausführt, wird der Begriff der identifizierten Person nicht näher erläutert.[155]

Grundsätzlich ist daher davon auszugehen, dass eine Person dann i.S.d. Art. 4 Nr. 1 identifiziert ist, wenn ohne Schwierigkeiten die Identität der Person aus der Information selbst ermittelt werden kann, etwa weil der Name oder die Anschrift bekannt sind. Insgesamt kann eine Person daher dann als identifiziert gelten, wenn keine zusätzlichen Informationen mehr notwendig sind, um die Person zu identifizieren[156] [157] [158]

Hinsichtlich der Frage, wann eine Person als identifizierbar einzustufen ist, äußert sich die DS-GVO in Art. 4 Nr. 1 demgegenüber ausdrücklich: Dies ist dann der Fall, wenn die Person direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung, wie einem Namen zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Entscheidend für das Merkmal einer Identifizierbarkeit ist somit, dass eine vorhandene Information als solche für eine Identifizierung nicht ausreicht, sondern diese vielmehr erst durch die Zuhilfenahme und Verknüpfung mehrerer Informationen miteinander ermöglicht wird.[159] [160]

Um festzustellen, ob eine Person identifizierbar ist, sind laut **Erwägungsgrund 26** S. 3[161] alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Bei diesen Mitteln sind nach **Erwägungsgrund 26**

155 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 3376 von 87533, Rn. 19.
156 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Art. 4 Nr. 1, Rn. 12.
157 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, Art. 4 Nr. 1, Rn. 17.
158 *Bäcker,* Datenschutz-Grundverordnung, Art. 4 Nr. 1, Rn. 18 f.
159 *Bäcker,* Datenschutz-Grundverordnung, Art. 4 Nr. 1, Rn. 18 DSGVO.
160 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 3242 von 87533, Rn. 9.
161 Amtsblatt der Europäischen Union 04.05.2016 (Erwägungsgrund 26 Satz. 4 DSGVO).

S. 4 alle Faktoren, wie Kosten und Zeitaufwand der Identifizierung sowie verfügbare Technologien und technologische Entwicklungen zu berücksichtigen, wobei dieser Katalog nicht abschließend ist. Daraus folgt, dass nach den Vorgaben der DS-GVO eine Abwägung erforderlich ist, bei der die Erfolgsaussichten einer Identifizierung in Relation zu Verhältnismäßigkeitserwägungen gesetzt werden.[162]

Fraglich ist insbesondere, wann unter rechtlichen Gesichtspunkten bzw. anhand welcher Maßstäbe eine „Identifizierbarkeit" der Person anzunehmen ist. Hierzu existieren im Ausgangspunkt zwei verschiedene Begründungsansätze: Ein relativer Ansatz stellt maßgeblich darauf ab, ob der für die Datenverarbeitung Verantwortliche anhand der ihm zur Verfügung stehenden Informationen und Mittel einen Personenbezug herstellen kann, während ein absoluter Ansatz es demgegenüber bereits genügen lässt, dass ein Dritter den Personenbezug herstellen könnte.[163]

Da weder die DS-GVO noch die **Erwägungsgründe**[164] in dieser Hinsicht eine eindeutige Aussage treffen, lässt sich die Frage, welches Verständnis Art. 4 Nr. 1 zugrunde liegt nur im Wege der Auslegung ermitteln: Der Wortlaut des **Erwägungsgrund 26** S. 3 nennt neben dem Verantwortlichen auch „andere Personen", was für ein weites Begriffsverständnis im Sinne eines **absoluten Ansatzes** spricht. Einschränkend verlangt **Erwägungsgrund 26** S. 3 aber, dass die Nutzung der Mittel „nach allgemeinem Ermessen wahrscheinlich" ist. Dies ist bei einem Dritten häufig dann der Fall, wenn dieser die personenbezogenen Daten selbst verarbeitet, so dass der Dritte selbst an der Identifizierung beteiligt sein muss.[165] Darüber hinaus spricht die in **Erwägungsgrund 26** angedeutete Notwendigkeit einer Verhältnismäßigkeitsprüfung für einen **relativen Ansatz**.[166]

---

162 *Bäcker,* Datenschutz-Grundverordnung, Art. 4 Nr. 1, Rn. 22 DSGVO.
163 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Art. 4 Nr. 1, Rn. 15 DSGVO.
164 Amtsblatt der Europäischen Union 04.05.2016 (ErwG - Erwägungsgründe DSGVO).
165 *Bäcker,* Datenschutz-Grundverordnung, Art. 4 Nr. 1, Rn. 26 DSGVO.
166 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 3376 von 87533, Art. 4 Nr. 1, Rn. 24 DSGVO.

Die Art.-29-Datenschutzgruppe geht ebenfalls davon aus, dass eine „rein hypothetische Möglichkeit der Herstellung eines Personenbezugs noch nicht ausreicht, um die Person als bestimmbar anzusehen“[167] und folgt damit ebenfalls einem relativen Verständnis.

Nach **teleologischen** Gesichtspunkten scheint eine absolute Betrachtungsweise darüber hinaus zu der widersprüchlich anmutenden Folge zu führen, dass datenverarbeitende Unternehmen grundsätzlich **jegliche Daten als personenbezogen ansehen müssten**, wenn es für die Identifizierbarkeit auch unter Umständen auf die (ungewisse) Kenntnis und Mittel Dritter ankäme. Eine derartige Rechtsunsicherheit in der Praxis kann im System des Datenschutzrechts nicht gewollt sein[168]. Denn in der Konsequenz würden die Unterschiede in den Begrifflichkeiten von „identifiziert“ und „identifizierbar“ faktisch eingeebnet und den Wortlaut der Verordnung sinnwidrig erscheinen lassen. Hinzu tritt, dass im Falle eines absoluten Ansatzes faktisch keine anonymisierten Daten mehr existieren könnten, so dass dieses Rechtsinstitut ebenfalls ausgehebelt würde.[169] Ergänzend lässt sich anführen, dass bei einem absoluten Verständnis des Art. 4 Nr. 1 auch rechtswidrig erlangte Kenntnisse und Mittel Dritter in die Betrachtung einbezogen würden.[170]

Auch der EuGH folgt in der Rechtssache Breyer gegen BRD[171] einem relativen Verständnis, indem er annimmt, dass „eine dynamische IP-Adresse, über die ein Nutzer die Internetseite eines Telemedienanbieters aufgerufen hat, für Letzteren ein personenbezogenes Datum [ist], soweit ein Internetzugangsanbieter über weitere zusätzliche Daten verfügt, die in Verbindung mit der dynamischen IP-Adresse die Identifizierung des Nutzers ermöglichen“. Gegenstand des Verfahrens war die Speicherung von IP-Adressen durch den Betreiber einer Webseite bei deren Aufruf. Der BGH hatte dem EuGH insbesondere die Frage vorgelegt, ob dynamische IP-Adressen ein

---

167 *Datenschutzgruppe 29,* Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, WP 136 zu „personenbezogenen Daten“, S. 17.

168 *Assion,* Kommentar Datenschutz-Grundverordnung, S. 58, Rn. 11, Artikel 4 Nr. 1 DSGVO.

169 *Assion,* Kommentar Datenschutz-Grundverordnung, S. 58, Rn. 11, Artikel 4 Nr. 1 DSGVO.

170 *Assion,* Kommentar Datenschutz-Grundverordnung, S. 58, Rn. 11, Artikel 4 Nr. 1 DSGVO.

171 Zweite Kammer, Urteil v. 19.10.2016, In der Rechtssache C-582/14, C 582/14 – „Vorlage zur Vorabentscheidung – Verarbeitung personenbezogener Daten – Richtlinie 95/46/EG – Art. 2 Buchst. a – Art. 7 Buchst. f – Begriff ‚personenbezogene Daten‘ – Internetprotokoll-Adressen – Speicherung durch einen Anbieter von Online-Mediendiensten – Nationale Regelung, die eine Berücksichtigung des berechtigten Interesses des für die Verarbeitung Verantwortlichen nicht zulässt“.

„personenbezogenes Datum“ seien, wenn der Internetzugangsanbieter über Zusatzwissen verfügt, mit dem eine Identifizierung des Besuchers ermöglicht wird.[172] Schon der Generalanwalt vertrat die Ansicht, dass eine IP-Adresse für den Telemedienanbieter ein personenbezogenes Datum sei, wenn der Internetzugangsanbieter über Zusatzwissen verfüge, um den Besucher der Internetseite zu identifizieren, wobei nur solche als „Dritte“ angesehen werden könnten, an die sich der Telemedienanbieter vernünftigerweise halten könne, um mit vernünftigem Aufwand deren zusätzliche Kenntnisse zu nutzen.[173] Der EuGH ist dem Generalanwalt im Wesentlichen gefolgt, indem er betont, dass eine dynamische IP-Adresse jedenfalls dann als personenbezogenes Datum einzustufen ist, wenn der Webseitenbetreiber über die rechtlichen Mittel verfügt, den Besucher der Internetseite mithilfe des Internetzugangsanbieters als Dritten zu bestimmen. Entscheidend ist somit die Perspektive des Verantwortlichen und die Identifizierbarkeit mithin danach zu bemessen, ob das Zusatzwissen Dritter für diesen zugänglich gemacht werden kann.[174]

Im Ergebnis ist daher eine vermittelnde Position vorzugswürdig, die eine Identifizierbarkeit maßgeblich von den Kenntnissen, Mitteln und Möglichkeiten des Verantwortlichen abhängig macht, indem dieser die Identifikation mit den ihm zur Verfügung stehenden Mitteln im Rahmen der o.g. Verhältnismäßigkeitserwägungen vornehmen kann.[175] Weil aber bei Licht betrachtet kaum Fälle denkbar sind, in denen man nach den vom EuGH aufgestellten Grundsätzen die Personenbeziehbarkeit ablehnen kann, kommt dessen relativer Ansatz einem absoluten faktisch sehr nahe.[176]

---

172 BGH - Bundesgerichtshof, 28. Oktober 2014 – VI ZR 135/13 Juris Bundesgerichtshof Entscheidungen.

173 *Generalanwalt EuGH*, Schlussanträge des Generalanwalts v. 12.5.2016 (1), Rechtssache C-582/14, Rn. 67 – „Verarbeitung personenbezogener Daten – Richtlinie 95/46/EG – Art. 2 Buchst. a und Art. 7 Buchst. f – Begriff ‚personenbezogeneDaten‘ – IP-Adressen – Speicherung durch einen Diensteanbieter für Telemedien – Nationale Regelung, die eine Berücksichtigung des berechtigten Interesses des für die Verarbeitung Verantwortlichen nicht zulässt“.

174 Zweite Kammer, Urteil v. 19.10.2016, In der Rechtssache C-582/14 – „Vorlage zur Vorabentscheidung – Verarbeitung personenbezogener Daten – Richtlinie 95/46/EG – Art. 2 Buchst. a – Art. 7 Buchst. f – Begriff ‚personenbezogene Daten‘ – Internetprotokoll-Adressen – Speicherung durch einen Anbieter von Online-Mediendiensten – Nationale Regelung, die eine Berücksichtigung des berechtigten Interesses des für die Verarbeitung Verantwortlichen nicht zulässt“.

175 *Assion,* Kommentar Datenschutz-Grundverordnung, S. 59, Rn. 12 Art. 4 Nr. 1 DSGVO.

176 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 3439, Rn. 28.

2.1.9 Anonyme Daten

Erwägungsgrund 26 S. 5 führt aus, dass die Grundsätze des Datenschutzes nicht für anonyme Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert wurden, dass die betroffene Person nicht mehr identifiziert werden kann, gelten. Folglich bilden laut den Vorgaben der Verordnung das personenbezogene Datum und das anonyme Datum Gegensätze. In der Folge fallen anonymisierte Daten – anders als pseudonymisierte – aus dem Anwendungsbereich der DS-GVO heraus.[177] Ob eine Person nicht mehr identifiziert werden kann, richtet sich nach den in Erwägungsgrund 26 S. 3 und 4 aufgeführten Maßstäben. Hinsichtlich der Frage, welche technischen Vorgaben an eine Anonymisierung zu stellen sind, trifft die DS-GVO auch in Erwägungsgrund 26 keine Aussage. Es kommen sowohl das Aggregieren von Daten als auch eine absolute, faktische oder formale Anonymisierung etwa durch das vollkommene Verschlüsseln von Daten oder das bloße Weglassen von Informationen, so dass eine Identifizierbarkeit ausscheidet, in Betracht.[178] [179]

177 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, S. 264, Art. 4 Nr. 1, Rn. 24 DSGVO.

178 *Bäcker,* Datenschutz-Grundverordnung, S. 132, Rn. 33 f. Art. 4 Nr. 1 DSGVO.

179 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Anonyme Daten, 3443 von 87533, Rn. 29.

2.2 Art. 4 Nr. 2 DS-GVO Verarbeitung

Unter „Verarbeitung“ versteht man jeden, mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.[180]

Ausgehend von dieser weiten Definition der Verarbeitung, die zur Folge hat, das jeder Umgang mit personenbezogenen Daten als ein Verarbeiten im Sinne der DS-GVO zu klassifizieren ist und damit einen datenschutzrechtlichen Tatbestand darstellt, muss der für die Verarbeitung Verantwortliche über eine Legitimation für die Verarbeitung verfügen.

Aufgrund des weiten Verarbeitungsbegriffs ist es aus Sicht des Rechtsanwenders ratsam, bei jedem Umgang mit personenbezogenen Daten von einer **Verarbeitung** i.S.d. DS-GVO auszugehen. Andernfalls drohen erhebliche Sanktionen nach Art. 82 ff. Die Verarbeitung bedarf immer einer Legitimierung. Zu beachten ist daneben, dass Auftragsverarbeitungen unter der DS-GVO nicht mehr privilegiert sind. Nach aktueller Rechtslage bedarf jede Auftragsverarbeitung einer gesetzlichen Erlaubnis. Bestehende Auftragsverarbeitungen sollten daher auf ihre Rechtmäßigkeit hin überprüft werden.[181]

180 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art.4 Nr.2 DSGVO.

181 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 3516 von 87533, Rn. 43.Praxishinweise.

2.3 Art. 4 Nr. 3 DS-GVO Einschränkung der Verarbeitung

Die Einschränkung der Verarbeitung nach Art. 4 Nr. 3 ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken. Die Verarbeitungseinschränkung ist ein zulässiges „Minus“ zum Löschen, wenn die personenbezogenen Daten für bestimmte Zwecke nach wie vor rechtmäßig verarbeitet werden dürfen. Inhaltlich entspricht die Einschränkung der Verarbeitung dem bisher gebräuchlichen „**Sperren**“ von Daten. Das Sperren war auch der DSRL nicht fremd, obgleich der Begriff dort nicht definiert war. Als eine Form der Verarbeitung personenbezogener Daten wurde das Sperren aber in Art. 2 lit. b ausdrücklich erwähnt. Im deutschen Datenschutzrecht definierte § 3 Abs. 4 Nr. 4 BDSG a.F. das Sperren als das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken. Diese Definition ist zwar nicht deckungsgleich mit der der DS-GVO. Sie ist aber bereits nah an der Definition der Einschränkung der Verarbeitung nach Art. 4 Nr. 3. Mit § 35 Abs. 1 und 2 BDSG n.F. hält auch der nationale Gesetzgeber an der Berechtigung des Verantwortlichen fest, anstelle einer Löschung eine Verarbeitungseinschränkung (früher: Sperrung) vorzunehmen.[182]

In automatischen Dateisystemen soll die Einschränkung der Verarbeitung grundsätzlich durch technische Mittel so erfolgen, dass die personenbezogenen Daten in keiner Weise weiterverarbeitet werden und nicht verändert werden können. (vgl. Erwägungsgrund 67)[183]

Erwägungsgrund 67:

Methoden zur Beschränkung der Verarbeitung personenbezogener Daten könnten unter anderem darin bestehen, dass ausgewählte personenbezogenen Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden, dass sie für Nutzer gesperrt werden oder dass veröffentliche Daten vorübergehend von einer Website entfernt werden. In automatisierten Dateisystemen sollte die Einschränkung der Verarbeitung grundsätzlich durch technische Mittel so erfolgen, dass die personenbezogenen Daten in keiner Weise weiterverarbeitet werden und nicht verändert werden können. Auf die Tatsache, dass die

182 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, 3558 von 87533, Rn. 44.

183 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Seite 37, Rn. 35.

Verarbeitung der personenbezogenen Daten beschränkt wurde, sollte in dem System unmissverständlich hingewiesen werden.[184]

2.4 Art. 4 Nr. 4 DS-GVO Profiling

Art. 4 Nr. 4 definiert „Profiling" als jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Es sind also Vorgänge gemeint, bei denen in der Regel größere Datenmengen zusammengeführt und automatisiert ausgewertet werden, wodurch beispielsweise besondere Vorlieben und Interessen oder Aufenthaltsorte einzelner betroffener Personen ermittelt werden können.[185] Unerheblich ist nach dem Wortlaut der Norm, ob die personenbezogenen Daten aus einer oder aus verschiedenen Quellen stammen. Ob der Verantwortliche einen oder mehrere Zwecke verfolgt oder ob die Bewertung der natürlichen Peron der Vorbereitung einer automatisierten Einzelfallentscheidung dient, ist ebenfalls nicht von Bedeutung.[186]

Ausweislich des **Erwägungsgrund 72** ist das Profiling eine Art der Verarbeitung personenbezogener Daten, die durch einen Erlaubnistatbestand der Art. 6 oder 9 legitimiert sein muss. Relevant ist die Norm damit vor allem für Verantwortliche, die automatisierte Einzelentscheidungen vornehmen und dabei Profilinganalysen oder –vorhersagen verwenden.[187]

Erwägungsgrund 72:

Das Profiling unterliegt den Vorschriften dieser Verordnung für die Verarbeitung personenbezogener Daten, wie etwa die Rechtsgrundlage für die Verarbeitung oder die

184 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 72.

185 *Laue/Kremer,* Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl. 2019, § 2 Rn. 84.

186 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 3627 von 87533, Rn. 54.

187 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 3627 von 87533, Rn. 55.

Datenschutzgrundsätze. Der durch diese Verordnung eingerichtete Europäische Datenschutzausschuss (im Folgenden "Ausschuss") soll diesbezüglich Leitlinien herausgeben können.

Der Verantwortliche muss den Betroffenen dann über ein Profiling informieren, wenn es zu einer automatisierten Entscheidungsfindung führt, Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g. Auf Antrag muss der Verantwortliche dem Betroffenen Auskunft über ein Profiling geben, aber ebenfalls nur bei einer damit in Zusammenhang stehenden automatisierten Entscheidungsfindung, Art. 15 Abs. 1 lit. h. Nach Art. 35 Abs. 3 lit. a kann eine Datenschutz-Folgenabschätzung bei automatisierten Einzelentscheidungen, die auf Profiling gründen, erforderlich sein.[188]

2.5 Art. 4 Nr. 5 DS-GVO Pseudonymisierung

In verschiedenen Disziplinen spielen die Begriffe „Pseudonymisierung“ und „Pseudonym“ eine Rolle, ohne dass es bisher einheitliche Definitionen gegeben hätte. Schon die Verwendung in verschiedenen juristischen Normen stellen auf verschiedene Qualitäten der Pseudonyme / Pseudonymisierung ab (beispielsweise im Signaturgesetz, im **T**ele**m**edien**g**esetz (**TMG**) oder im alten LDSG Schleswig-Holstein). Ähnliches gilt für die Annäherung an das Thema aus technischer Sicht. In der vorliegenden Betrachtung soll zwar primär auf die DS-GVO-Definition zu Pseudonymisierung Bezug genommen werden, jedoch garantieren die technischen Verfahren, die mehr oder weniger für eine Pseudonymisierung geeignet sein können, allein häufig noch nicht, dass die Anforderungen an eine Pseudonymisierung im Sinne der DS-GVO erfüllt werden. Dies kann zudem von weiteren Faktoren abhängen wie beispielsweise von den zu pseudonymisierenden Daten selbst oder etwaigem Zusatzwissen. Dies vorausgeschickt, nehmen wir einen Blick in die Definition in Art. 4 Nr. 5 der DS-GVO.[189]

„Pseudonymisierung“ ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und **t**echnischen und

188 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, 3666 von 87533, Rn.61 Pflichten beim Profiling.

189 *Hansen, Marit / Walcza, Benjamin* RDV / Recht der Datenverarbeitung Heft 2/2019 (53).

organisatorischen **M**aßnahmen (**TOM**) unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;[190]

Zentral für die Anwendung des Datenschutzrechts ist der Personenbezug von Daten (vgl. Art. 4 Nr. 1 Rn. 1 DS-GVO). Gemäß dem Prinzip des Datenschutzgrundsatzes sowie der Datenminimierung (ebenfalls Art. 5 Abs. 1 lit. c Rn. 116 ff. DS-GVO) müssen die verarbeiteten Daten auf, das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Mithilfe von Anonymisierung oder Pseudonymisierung ist es im Sinne der Datenminimierung möglich, personenbezogene Daten so zu verändern, dass der Personenbezug nicht mehr bzw. nur bei Hinzuziehen **weiterer** Informationen hergestellt werden kann. [191]

Die Pseudonymisierung muss als ein Mittel der **Risikominimierung** gesehen werden. Zu Recht macht Erwägungsgrund 28[192] deutlich, dass es sich bei diesem Verfahren nicht um die einzige Möglichkeit der grundrechtsschonenden Datenverarbeitung handelt.[193]

Darüber hinaus weist die Pseudonymisierung eine enge Verknüpfung mit dem Datenschutzprinzip des „**Privacy by Design**" aus Art. 25 auf. Sie sorgt dafür, dass bereits in einem frühen Stadium durch **t**echnisch-**o**rganisatorische **M**aßnahmen (**TOM**) eine Entkoppelung persönlicher Informationen von anderen Daten erfolgen kann, was zu einem wirksamen Schutz für die Betroffenen führt. Im Rahmen eines risikobasierten Ansatzes wirkt sich die Pseudonymisierung auch zugunsten des Verantwortlichen aus. So kann sie Verarbeitungen zulässig machen, die ansonsten unzulässig wären. Dies ist insbesondere im Zeitalter von **Big Data** und **Internet of Things** von wesentlicher Bedeutung. Ein wichtiges Anwendungsbeispiel ist dabei Art. 6 Abs. 4, der für eine Datenverarbeitung im Falle einer Zweckänderung gilt: Ob der neue (geänderte) Verarbeitungszweck mit dem ursprünglichen Zweck der Datenerhebung / -verarbeitung vereinbar ist, entscheidet eine Abwägung. Ein wichtiges Kriterium im Rahmen dieser

190 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 5 DSGVO.

191 *J. Philipp Albrecht,* Datenschutzrecht, Seite 311. Rn.1.

192 Amtsblatt der Europäischen Union 04.05.2016 (Erwägungsgrund 28 DSGVO).

193 *Assion,* Kommentar Datenschutz-Grundverordnung, Seite 82. Rn. 2 Regelungszweck.

Kompatibilitätsprüfung ist das Vorhandensein geeigneter Garantien, wozu auch die Pseudonymisierung zählt.[194]

Erwägungsgrund 28

Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann die Risiken für die betroffenen Personen senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen. Durch die ausdrückliche Einführung der "Pseudonymisierung" in dieser Verordnung ist nicht beabsichtigt, andere Datenschutzmaßnahmen auszuschließen.[195]

194 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, 3712 von 87533, Rn. 67.

195 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 28.

2.6 Big Data

Mit „Big Data“ werden große Mengen an Daten bezeichnet, die u.a. aus Bereichen wie Internet und Mobilfunk, Finanzindustrie, Energiewirtschaft, Gesundheitswesen, Verkehr und aus Quellen wie intelligenten Agenten, sozialen Medien, Kredit- und Kundenkarten, Smart-Metering-Systemen (computergestützte Messen, Ermitteln und Steuern von Energieverbrauch und -zufuhr), Assistenzgeräten, Überwachungskameras sowie Flug- und Fahrzeugen stammen und die mit speziellen Lösungen zu Zwecken der (Inter-)Dependenzanalyse, Umfeld- und Trendforschung sowie zu System- und Produktionssteuerungszwecken gespeichert, verarbeitet und ausgewertet werden.[196]

Zahlreiche Unternehmen bauen ihr Geschäft auf der Grundlage verschiedenster Technologien auf, die es ermöglichen, umfangreiche Datensätze zu erheben, zu verarbeiten, zu kategorisieren und zu analysieren, um auf diese Weise die Daten (wirtschaftlich) zu verwerten zu können. Dabei bezieht sich der Begriff „Big Data“ eher auf einen speziellen Datenverarbeitungsansatz, als auf bestimmte Verarbeitungstechniken. Derartige Big Data-Anwendungen verarbeiten häufig lediglich sachbezogene Daten, wie über das Wetter oder zu Maschinenabläufen, aber zunehmend auch große Mengen personenbezogener Nutzerinformationen, um menschliches Verhalten zu verstehen, vorauszusagen und zu lenken.

Typische Big Data-Aktivitäten bestehen im Tracking von natürlichen Personen, zur Vermeidung von Streuverlusten bei Werbemaßnahmen, sowie in Analysen und Vorhersagen zu Nutzerverhalten, weshalb die personenbezogenen Daten zu einem wertvollen Wirtschaftsgut geworden sind. Solche Tätigkeiten lassen sich in zwei Kategorien einteilen: Verhaltensanalysen auf einem „Makro-Level“ in Bezug auf Personengruppen und Verhaltensanalysen in Bezug auf Einzelpersonen, also sozusagen auf „Mikro-Level“. Vor allem **Profiling** wurde vom europäischen Gesetzgeber als besonders kritische Verarbeitungstätigkeit eingestuft und ist deswegen Gegenstand einer Sondervorschrift, vgl. Art. 22 DS-GVO.[197]

196 *Caldarola/Schrey,* Big Data und Recht, 2019, Seite.1, Rn. 1.
197 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, Position 9778 von 14106, Abschnitt: 9.1 Big Data.

Big Data wie auch die einzelnen Daten selbst werden daher heute oft als das „**Öl des 21.Jahrhunderts**“ bezeichnet.[198]

Daten sind Werte und Befunde über Dinge, Ereignisse, Personen und Zustände, die durch Beobachtung und Messung ermittelt werden und in ihrer Formulierung technisch entweder elektronisch oder auch körperlich festgehalten werden.[199]

In diesem Zusammenhang spielen Datenbanken eine wichtige Rolle, denn Big Data-Anwendungen basieren auf großen Datenbanken, in denen die verschiedensten Daten aus den unterschiedlichsten Quellen gesammelt und geordnet abgelegt werden. Datenbanken sind Sammlungen von Einzelinformationen, die systematisch bzw. methodisch angeordnet sind. In Datenbanken können personenbezogen, technische und / oder anonyme Daten enthalten sein.[200]

Eine Datenbank im Sinne von § 87a UrhG ist eine Sammlung von Werken, Daten, Einzelinformationen oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit elektronischen Mitteln oder auf andere Weise zugänglich ist.[201]

So einig man sich über die Begriffsbestimmung und das Bedürfnis nach praktischer Anwendung ist, so weitreichend und unterschiedlich sind die datenschutzrechtlichen Herausforderungen, die mit Big Data-Verfahren einhergehen. Das Datenschutzrecht wird in der Wirtschaft noch immer als Einsatzhemmnis für Big Data Projekte gesehen. Die große Frage ist, ob sich dieser Zustand durch die Einführung der DS-GVO eher manifestiert hat oder entspannen wird. Für Ersteres sprechen gewichtige Argumente. Im November 2015 hat der Europäische Datenschutzbeauftragte (EDSB) Giovanni Buttarelli die Stellungnahme „Meeting the challenges of big data – A call for transparency, user control, Data Protection by Design and accountability“[202] veröffentlicht. Es lässt sich aber

198 *Caldarola/Schrey,* Big Data und Recht, 2019, Seite. 1, Rn. 2.
199 *Caldarola/Schrey,* Big Data und Recht, 2019, Seite. 1 Rn. 5.
200 *Caldarola/Schrey,* Big Data und Recht, 2019, Seite. 2 Rn. 7.
201 *Caldarola/Schrey,* Big Data und Recht, 2019, Seite. 22+23, Rn. 65 Datenbankschutzrecht.
202 *Buttarelli, Giovanni*, Meeting the challenges of big data, A call for transparency, user control, data protection by design and accountability 07.2015, https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf.

nicht entnehmen, dass insoweit noch Restriktionen Eingang in die DS-GVO gefunden hätten. Im Gegenteil: „Big Data“ kommt in der DS-GVO **schlicht nicht vor**.[203]

Das Datenschutzrecht – so auch die DS-GVO – setzt einen Personenbezug der zu verarbeitenden Daten voraus. Dort, wo Big Data-Anwendungen Daten ohne jeden Personenbezug (anonyme Daten) analysieren, findet das Datenschutzrecht keine Anwendung. „Big Data heißt nicht notwendig Big Personal Data."[204]. Die Zusammenführung verschiedenster Daten zu großen Datenmengen erleichtert jedoch potenziell die Aufhebung von Anonymität.[205]

2.7 Art. 4 Nr. 6 DS-GVO Dateisystem

„Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.[206]

Die Definition des Dateisystems entspricht in der englischen Fassung vollständig, in der deutschen nahezu wörtlich der Definition in Art. 2 lit. c DSRL. Mit Ausnahme der Ersetzung der Bezeichnung Datei durch die des Dateisystems und des Wortes „**gleichgültig**“ durch die Worte „**unabhängig davon**“ sind die Definitionen der DSRL und der DS-GVO identisch.[207]

Zudem müssen nach Art. 4 Nr. 6 die Daten und Einzelangaben nach bestimmten personenbezogenen Kriterien zugänglich sein. Das Kriterium bezeichnet dabei die Merkmale und Kategorien (etwa Name, Beruf, Alter oder Anschrift einer Person), anhand derer die Daten zugänglich gemacht werden. Zugänglich sind die Daten und Einzelangaben dann, wenn sie anhand der Merkmale und Kategorien inhaltlich

---

203 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 11048 von 87533, Rn.229.

204 Holger Nohr, in: *Big Data im Lichte der EU-Datenschutz-Grundverordnung*, siehe auch Dix, S.60.

205 Holger Nohr, in: *Big Data im Lichte der EU-Datenschutz-Grundverordnung*, siehe auch Dix, S. 61 und Boehme-Neßler 2016.

206 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 6 DSGVO.

207 *J. Philipp Albrecht,* Datenschutzrecht, Seite.324, Rn.3, Datenschutz-Richtlinie.

erschlossen und verfügbar gemacht werden können. Aufgrund der heutigen technischen Möglichkeiten ist daher davon auszugehen, dass jede Form der geeigneten und strukturierten Speicherung von Daten, die eine Auswertung anhand verschiedener Kriterien ermöglicht, als Dateisystem im Sinne des Art. 4 Nr. 6 anzusehen ist. So fallen etwa Personenverzeichnisse oder alphabetische Sortierungen unter die Begriffsdefinition. Auch Akten oder Aktensammlungen unterfallen laut Erwägungsgrund 15 S. 3 der DS-GVO, sofern sie die Begriffsdefinition des Dateisystems erfüllen.

In der Praxis ist insbesondere die Frage bedeutsam, ob die Digitalisierung von ursprünglich nur in Papierform bestehenden Daten und Akten unter die Begriffsdefinition des „Dateisystems" nach Art. 4 Nr. 6 fällt. Nach **Erwägungsgrund 15** S. 3[208] fallen Akten oder Aktensammlungen, die nicht nach bestimmten Kriterien geordnet sind, nicht in den Anwendungsbereich der DS-GVO. Entscheidend ist deshalb, ob im Rahmen der Digitalisierung von Datenbeständen Ordnungskriterien erstellt werden, die die personenbezogenen Daten zugänglich machen. Sofern die Daten und Akten lediglich als solches eingescannt und abgelegt werden, wird dies nicht der Fall sein. Sobald aber die Dokumente nach einem vorher festgelegten Ordnungsschema abrufbar sind, kann sich die Beurteilung ändern.[209]

Erwägungsgrund 15

Um ein ernsthaftes Risiko einer Umgehung der Vorschriften zu vermeiden, sollte der Schutz natürlicher Personen technologieneutral sein und nicht von den verwendeten Techniken abhängen. Der Schutz natürlicher Personen sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung von personenbezogenen Daten, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, sollten nicht in den Anwendungsbereich dieser Verordnung fallen[210]

208 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

209 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, 3973 von 87533, Rn. 97.

210 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 15.

2.8 Art. 4 Nr. 7 DS-GVO Verantwortlicher

Als Verantwortlicher werden natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen bezeichnet, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Sind Zweck und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.[211]

Der Begriff des Verantwortlichen (sowie die damit eng verbundenen weiteren Begrifflichkeiten des Auftragsverarbeiters und Dritten) dienen nach Ansicht der Art. 29-Datenschutzgruppe „in erster Linie dazu, zu bestimmen, wer für die Einhaltung der Datenschutzbestimmungen verantwortlich ist und wie die betroffenen Personen ihre Rechte in der Praxis ausüben können. Anders ausgedrückt: Er dient dazu, Verantwortung zuzuweisen." Dazu werden in dieser Norm die möglichen Adressaten der Qualifikationen als Verantwortlicher und vor allem das entscheidende Abgrenzungsmerkmal definiert.[212]

Der „Verantwortliche" stellt einen der zentralen Begriffe der DS-GVO[213] dar. Besondere Bedeutung hat die Begrifflichkeit insbesondere im Rahmen der Art. 5 Abs. 2, 24, 26 und 28 DS-GVO. Art. 5 Abs. 2 betrifft die Rechenschaftspflicht des Verantwortlichen. Art. 24 beschreibt die grundsätzliche Verantwortung des Verantwortlichen und der Auftragsverarbeiter. Art. 26 nimmt auf die Begrifflichkeit der gemeinsam Verantwortlichen Bezug, während Art. 28 die Abgrenzung zum Auftragsverarbeiter und dessen Aufgabenkreis betrifft.[214]

---

211 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art.4 Nr.7 DSGVO.

212 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, Seite. 148, Rn. 1.

213 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).

214 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position. 3999 von 87533, Rn. 103.

Nach Art. 4 Nr. 7[215] ist es für die Zuweisung der Verantwortlicheneigenschaft nicht notwendig, dass der Verantwortliche ausschließlich allein Daten verarbeitet. Vielmehr kann nach der DS-GVO die Entscheidung über Zwecke und Mittel der Datenverarbeitung „allein oder gemeinsam mit anderen" getroffen werden, indem bei der Verarbeitung personenbezogener Daten mehrere Akteure beteiligt sind und somit verschiedene Verantwortliche bestehen. Die DS-GVO greift damit insbesondere auch mit Blick auf Art. 26 die Begrifflichkeit und Systematik von Art. 2 lit. d DSRL auf.[216]

Noch nicht abschließend geklärt und Anfang 2018 auf europäischer Ebene zur Debatte stand die datenschutzrechtliche Mitverantwortlichkeit der Betreiber von Fanpages bei Facebook.[217] Die Art. 29-Datenschutzgruppe vertritt in ihrem WP 169 die Position, dass derjenige, der weder unter rechtlichen noch tatsächlichen Gesichtspunkten Einfluss auf die Entscheidung der Verarbeitung personenbezogener Daten hat, nicht als Verantwortlicher angesehen werden kann.[218] Unter Bezug darauf legte das BVerwG im Rahmen eines Revisionsverfahrens dem EuGH die Frage zur Vorabentscheidung vor.[219] Der Generalanwalt vertritt in seinem Schlussbericht, dass der Betreiber der Fanpage und Facebook als gemeinsame Verantwortliche einzustufen ist. Facebook entscheide über die Ziele und Modalitäten der Datenverarbeitung und habe das Geschäftsmodell als solches entwickelt und der Betreiber der Fanpage schließe sich durch die Nutzung der Fanpage auf Facebook dieser Durchführung der Verarbeitung personenbezogener Daten an. Sollte der EuGH dem folgen, so hätte dies in datenschutzrechtlicher Hinsicht weitreichende Konsequenzen für die Betreiber von Fanpages im Rahmen von Social Media.[220]

Ebenfalls nicht geklärt ist die Frage, welche Folgen eine „aufgedrängte Verantwortlichkeit" hat. In diesen Situationen werden einem Dritten personenbezogene

---

215 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 7 DSGVO.

216 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 4133 von 87533, Rn. 116.

217 *Schwartmann/Keber/Mühlenbeck,* Social Media, 2. Aufl. 2018, S. 86 f.

218 *Datenschutzgruppe 29,* Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, Art.-29-Datenschutzgruppe WP 169 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 11 ff.

219 Bundesverwaltungsgericht, BVerwG 1 C 28.14 (25.02.2016).

220 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 4233, Rn. 123.

Daten z.B. offengelegt, ohne dass er hiervon Kenntnis hat oder dies will. Zu denken ist insbesondere an Fälle von Datenpannen, bei denen ein Verantwortlicher personenbezogene Daten, ob gewollt oder nicht, an die falsche Person übermittelt. Würde man den Dritten in diesen Situationen als Verantwortlichen einstufen, träfen ihn die kompletten Pflichten, die sich aus der DS-GVO für den Verantwortlichen ergeben. Resultierend aus der weiten Definition der Verarbeitung unter der DS-GVO verarbeitet der Dritte bereits bei Kenntnisnahme der personenbezogenen Daten dieselben. Unabhängig davon, ob auch eine aufgedrängte Verarbeitung unter die Begriffsdefinition des Art. 4 Nr. 7 zu fassen ist, erscheint es unbillig, würde man den Dritten in solchen Fallkonstellationen mit den Verpflichtungen eines Verantwortlichen belasten.[221]

Der Dritte hat keine Entscheidungsbefugnis über Zweck und Mittel der Verarbeitung. Er bekommt die Verarbeitung gegen seinen Willen aufgedrängt. Kontextbezogen betrachtet wird man in dieser Situation erkennen, dass der Dritte das Ob, Warum und Wie der Verarbeitung der personenbezogenen Daten nicht festlegt. Untermauert wird dieses Ergebnis auch dadurch, dass im Fall der Datenpanne der Verantwortliche zur Meldung der Panne verpflichtet ist, nicht der Dritte, der die Daten empfängt. Erst dann, wenn der Dritte die personenbezogenen Daten bewusst für eigene Zwecke verarbeitet, wird er zum Verantwortlichen nach der DS-GVO.[222]

221 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 4180 von 87533, Rn. 123.

222 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 4180 von 87533, Rn. 124.

2.9 Art. 4 Nr. 8 DS-GVO Auftragsverarbeiter

Der Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.[223]

Die Begriffsbestimmung des Auftragsverarbeiters nach Art. 4 Nr. 8 DS-GVO ist im engen Zusammenhang mit der Definition des Verantwortlichen nach Art. 4 Nr. 7 DS-GVO zu sehen. Beide Begriffe diesen in erster Linie dem Zweck, an einem Datenverarbeitungsvorgang beteiligte Akteure im Hinblick auf die Verantwortlichkeit zur Einhaltung diesbezüglicher einschlägiger datenschutzrechtlicher Vorschriften voneinander abzugrenzen. Auftragsverarbeiter können so von Verantwortlichen mit der Verarbeitung personenbezogener Daten beauftragt werden, ohne hierfür (umfassende) datenschutzrechtliche Verantwortlichkeit tragen zu müssen.[224]

Im deutschen Datenschutzrecht wurde bisher der Begriff der Funktionsübertragung als Gegenbegriff zur weisungsgebundenen Auftragsverarbeitung gebraucht. Eine Funktionsübertragung wurde angenommen, wenn der Dritte über eine eigene Entscheidungsbefugnis hinsichtlich des „Wie“ der Datenverarbeitung und diesbezüglich auch die Auswahlbefugnis hat, ihm damit die Aufgabe der Verarbeitung obliegt und er insoweit für die Datenverarbeitung verantwortlich ist und über die Daten verfügen kann. Der Dritte hat in diesem Fall ein eigenes Interesse an den Daten.

In Bezug auf freiberufliche Tätigkeiten, wie die eines Steuerberaters oder Wirtschaftsprüfers, wird man davon ausgehen müssen, dass eine Auftragsdatenverarbeitung regelmäßig nicht in Betracht kommt. Freiberufliche Tätigkeiten werden unabhängig, selbstständig und eigenverantwortlich durchgeführt. Diese Merkmale widersprechen grundlegend einer Weisungsgebundenheit, wie sie für die Auftragsverarbeitung elementar ist. So erläutert die Art. 29-Datenschutzgruppe auch bezogen auf den Rechtsanwalt, dass solche Berufsstände als unabhängige „für die

223 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 8 DSGVO.

224 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Seite.154, Rn.204.

Verarbeitung Verantwortliche“ anzusehen sind, wenn sie im Rahmen der rechtlichen Vertretung ihrer Klienten Daten verarbeiten.[225]

Der Begriff der Funktionsübertragung ist der DS-GVO fremd. Um sachgerechte Abgrenzungen vorzunehmen, wird aber am Konstrukt der Funktionsübertragung festzuhalten sein. Es ist auch weiterhin davon auszugehen, dass Rechtsanwälte, Steuerberater und andere freie Berufsträger und Dienstleister, die eine eigenverantwortliche und weisungsfreie Aufgabe übernehmen, selbst Verantwortliche und eben keine Auftragsverarbeiter sind. Sie bedürfen damit einer eigenen Legitimation zur Datenverarbeitung und haben die weiteren Pflichten eines Verantwortlichen zu erfüllen.[226]

2.10 Art. 4 Nr. 9 DS-GVO Empfänger

Ein „Empfänger“ ist gemäß Datenschutz-Grundverordnung, eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.[227]

Der Begriff des „Empfängers“ ist der Oberbegriff für alle Stellen, die personenbezogene Daten durch den Verantwortlichen erhalten. In der DS-GVO findet der Begriff insbesondere bei den Rechten des Betroffenen auf Information, Auskunft, Berichtigung und Löschung gemäß den Art. 13, 14, 15 und 19 DS-GVO Anwendung. Auch für das

225 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 4400 von 87533, Rn. 134.

226 *Assion,* Kommentar Datenschutz-Grundverordnung, Kramer, S. 95, Rn. 20.

227 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 9 DSGVO.

Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 ist der Begriff des Empfängers von Bedeutung.[228]

Adressat der Norm ist zunächst der Verantwortliche. Wenn er personenbezogene Daten einem Empfänger offengelegt hat, treffen ihn Informations- und Auskunftspflichten gegenüber dem Betroffenen, Mitteilungspflichten gegenüber dem Empfänger und Dokumentationspflichten.[229] Zusätzlich ist die Norm auch für den Empfänger der personenbezogenen Daten von Bedeutung. Dieser muss prüfen, ob und welche Pflichten ihn nach der DS-GVO treffen, sofern er als Empfänger einzustufen ist.[230]

Der Empfänger gehört mit dem Verantwortlichen (Art. 4 Nr. 7), dem Auftragsverarbeiter (Art. 4 Nr. 8), dem Dritten (Art. 4 Nr. 10), dem Betroffenen (Art. 4 Nr. 1) und dem Vertreter (Art. 4 Nr. 17) zu den Personen, denen durch die DS-GVO bei der Verarbeitung personenbezogener Daten eine mit Rechten und Pflichten versehene Rolle zugedacht ist.[231]

Art. 4 Nr. 9 S. 2 DS-GVO enthält eine Ausnahme von der Einordnung als Empfänger. Danach sollen Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach Unionsrecht oder dem Recht der Mitgliedstaaten personenbezogene Daten erhalten, nicht als Empfänger gelten. Der Begriff des Untersuchungsauftrags dürfte nach der deutschen Gesetzesterminologie am ehesten mit „Ersuchen“ übersetzt werden können.[232]

Erwägungsgrund 31 nennt beispielhaft und nicht abschließend die Steuer- und Zollbehörden, Finanzermittlungsstellen, unabhängige Verwaltungsbehörden oder Finanzmarktbehörden, die für die Regulierung von Wertpapiermärkten zuständig sind. Mangels Empfängereigenschaft entfallen hier die Informations- und Mitteilungspflichten. Art. 4 Nr. 9 S. 2 stellt jedoch klar, dass die Verarbeitung durch die

228 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 4462 von 87533, Rn. 140.
229 *Assion,* Kommentar Datenschutz-Grundverordnung, Kramer, S. 92, Rn. 5.
230 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 4462 von 87533, Rn. 141.
231 *Assion,* Kommentar Datenschutz-Grundverordnung, S. 109, Rn. 7,Systematik.
232 *Assion,* Kommentar Datenschutz-Grundverordnung, Veil, S. 113, Rn. 28.

ausgenommenen Behörden im Einklang mit den geltenden Datenschutzvorschriften erfolgen muss.[233]

Grund für die Privilegierung dieses Sachverhalts ist, dass die Verarbeitung durch die genannten Behörden ohnehin im Einklang mit den Datenschutzvorschriften der DS-GVO und des bereichsspezifischen Rechts zu erfolgen hat.[234]

Erwägungsgrund 31

Behörden, gegenüber denen personenbezogene Daten aufgrund einer rechtlichen Verpflichtung für die Ausübung ihres offiziellen Auftrags offengelegt werden, wie Steuer- und Zollbehörden, Finanzermittlungsstellen, unabhängige Verwaltungsbehörden oder Finanzmarktbehörden, die für die Regulierung und Aufsicht von Wertpapiermärkten zuständig sind, sollten nicht als Empfänger gelten, wenn sie personenbezogene Daten erhalten, die für die Durchführung - gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten - eines einzelnen Untersuchungsauftrags im Interesse der Allgemeinheit erforderlich sind. Anträge auf Offenlegung, die von Behörden ausgehen, sollten immer schriftlich erfolgen, mit Gründen versehen sein und gelegentlichen Charakter haben, und sie sollten nicht vollständige Dateisysteme betreffen oder zur Verknüpfung von Dateisystemen führen. Die Verarbeitung personenbezogener Daten durch die genannten Behörden sollte den für die Zwecke der Verarbeitung geltenden Datenschutzvorschriften entsprechen.[235]

233 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 4512 von 87533.

234 *Assion,* Kommentar Datenschutz-Grundverordnung, Veil, S. 113, Rn. 30.

235 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 31.

2.11 Art. 4 Nr. 10 DS-GVO Dritter

Nach Art. 4 Nr. 10 ist „Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.[236]

Die Definition des „Dritten“ stellt klar, welche Personen oder Stellen außerhalb der Verarbeitung personenbezogener Daten durch den Verantwortlichen stehen. Im Übrigen ist unklar, ob der „Dritte“ in der DS-GVO noch dieselbe Bedeutung hat, die ihm nach dem BDSG zukam.[237] Die Feststellung, ob jemand Dritter ist, kann positiv, insbesondere aber negativ vorgenommen werden.

Dritter kann eine natürliche oder juristische Person, eine Behörde, eine Einrichtung oder eine andere Stelle sein. Wie sich aus der Regelung des Art. 6 Abs. 1 lit. f. entnehmen lässt, muss es sich bei dem Dritten um eine Person oder Stelle handeln, dessen Interesse vom berechtigten Interesse des Verantwortlichen abweicht. Werden dem Dritten personenbezogene Daten offengelegt, wird er zum Empfänger und damit zum Verantwortlichen.

Art. 4 Nr. 10 grenzt den Dritten negativ ab. Danach ist der Dritte kein Betroffener, kein Verantwortlicher, kein Auftragsverarbeiter und keine Person, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt ist, personenbezogene Daten zu verarbeiten. Zum Auftragsverarbeiter gehören auch dessen Unterauftragnehmer.[238]

Maßgebliches Kriterium ist, dass der Dritte „außerhalb der verantwortlichen Stelle“ steht. Dritter ist damit in Abgrenzung zu einer Behörde jede andere Behörde, auch wenn diese zum gleichen Rechtsträger gehört. Damit ist auch jede andere öffentliche Stelle Dritter.

---

236 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 10 DSGVO.

237 *Assion,* Kommentar Datenschutz-Grundverordnung, S. 115 / 116, Rn. 1/2.

238 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 4557 von 87533, Rn. 154/155/156.

Innerhalb einer Behörde (z.B. Gemeindeverwaltung) können jedoch, wenn funktional mehrere Aufgaben wahrgenommen werden, die „Ämter“ dieser Behörde „Dritte“ zueinander sein. Dritte sind Personen oder Stellen, die mit dem Verantwortlichen nicht identisch sind. In dem Moment, in dem eine Person oder Stelle verantwortlich wird, ist sie nicht mehr Dritter. Beschäftigte des Verantwortlichen, die nicht befugt sind, personenbezogene Daten zu bearbeiten sind damit als Dritte einzustufen. Gibt also ein Mitarbeiter rechtswidrig personenbezogene Daten an einen Kollegen weiter, so ist darin eine **rechtswidrige Übermittlung** eines Dritten zu sehen.[239]

239 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 4616 von 87533, Rn. 156.

2.12 Art. 4 Nr. 11 DS-GVO Einwilligung

Art. 4 Nr. 11 definiert die „Einwilligung“ der betroffenen Person jede, freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.[240]

Die Einwilligung der betroffenen Person ist einer der Rechtsgründe für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten (Art. 6 Abs. 1).[241]

Um gültig zu sein, muss gemäß **Erwägungsgrund 32** die Einwilligung als Willensbekundung der betroffenen Person in informierter Weise erfolgen, freiwillig gegeben werden und unmissverständlich in Form einer Erklärung oder eindeutig bestätigenden Handlung Geschehen.[242]

Erwägungsgrund 32:

Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung. Dies könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen. Die Einwilligung sollte sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge beziehen. Wenn die Verarbeitung mehreren

240 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 11 DSGVO.

241 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, S. 247, Rn. 34.

242 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, S. 247, Rn. 35.

Zwecken dient, sollte für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden. Wird die betroffene Person auf elektronischem Weg zur Einwilligung aufgefordert, so muss die Aufforderung in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgen.[243]

Im deutschen Recht war die Einwilligung bisher in § 4a BDSG a.F. geregelt. Für eine nationale Regelung bleibt unter DS-GVO kein Raum mehr. Die Einwilligung hat nunmehr den Vorgaben der DS-GVO zu genügen. Lediglich in Bezug auf die Einwilligung im Beschäftigtenkontext lässt die DS-GVO über Art. 88 dem nationalen Gesetzgeber Regelungskompetenz. Hiervon wurde mit § 26 Abs. 2 BDSG n.F. Gebrauch gemacht.[244]

2.12.1 Wesentliche Elemente der Einwilligung

1. Die Freiwilligkeit, die erfordert, dass der Betroffene die Einwilligung frei von Zwang und ohne Kopplung an ein Rechtsgeschäft verlangt wird, nicht erforderlich sind,
2. Die Bestimmtheit, nach der beim Erteilen der Einwilligung feststehen muss, zu welchem konkreten Zweck und zu welcher konkreten Verarbeitung die Zustimmung erfolgt,
3. Die Informiertheit, die eine vorausgehende Unterrichtung des Betroffenen über den vorgesehenen Zweck und die Verarbeitung erfordert,
4. die Unmissverständlichkeit, die erfordert, dass der Betroffene eine eindeutige Willenserklärung abgibt.[245]

243 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 32.

244 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 4615 von 87533, Rn.161.

245 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Seite. 95, Rn.96, Wesentliche Elemente.

2.12.2 Weitere Voraussetzungen

Allerdings enthält Art. 4 Nr. 11 DS-GVO nicht sämtliche Voraussetzungen einer wirksamen Einwilligungserklärung. Weitere Voraussetzungen finden sich insbesondere in Art. 6 Abs. 1 lit. a und Art. 7 DS-GVO sowie ggf. in Art. 9 Abs. 2 lit. a (Verarbeitung besonderer Kategorien personenbezogener Daten), Art. 22 Abs. 2 lit. c (automatische Entscheidungen im Einzelfall) und Art. 49 Abs. 1 Satz 1 lit. a DS-GVO (Übermittlung personenbezogener Daten in ein Drittland). Durch diese, teilweise unnötige, Aufteilung hat der Verordnungsgeber die Verständlichkeit der DS-GVO und der Voraussetzung für eine wirksame Einwilligungserklärung leider erschwert. Für Einwilligung im Beschäftigungsverhältnis ist insbesondere auch § 26 Abs. 2 BDSG zu beachten.[246]

Im behördlichen Bereich ist die Einwilligung als Erlaubnis für die Verarbeitung selten anzutreffen. Zum einen wird das Verhältnis zwischen Bürger und staatlichen Stellen maßgeblich durch Gesetze geprägt (im Unterschied dazu herrscht Privatautonomie im Verhältnis zwischen Verbrauchern und Unternehmen, weshalb die Einwilligung in diesem Verhältnis eine große Bedeutung hat als im behördlichen Bereich) und zum anderen ist das Verhältnis zwischen Bürger und Behörde häufig von einem Ungleichgewicht geprägt, was besonders am Beispiel der Eingriffsverwaltung deutlich wird, von daher ist dort eine freiwillige Einwilligung in vielen Fällen nicht möglich (vgl. hierzu nachfolgenden **Erwägungsgrund 42**).[247]

Erwägungsgrund 42

Erfolgt die Verarbeitung mit Einwilligung der betroffenen Person, sollte der Verantwortliche nachweisen können, dass die betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat. Insbesondere bei Abgabe einer schriftlichen Erklärung in anderer Sache sollten Garantien sicherstellen, dass die betroffene Person weiß, dass und in welchem Umfang sie ihre Einwilligung erteilt. Gemäß der Richtlinie 93/13/EWG des Rates sollte eine vom Verantwortlichen vorformulierte Einwilligungserklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden, und sie sollte keine

246 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Einwilligung, Art. 4 Nr. 11 DSGVO, S. 169 Rn. 259.

247 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Seite. 95, Rn. 98.

missbräuchlichen Klauseln beinhalten. Damit sie in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen. Es sollte nur dann davon ausgegangen werden, dass sie ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.[248]

248 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 42.

2.13 Art. 4 Nr. 12 DS-GVO Verletzung des Schutzes personenbezogener Daten

Art. 4 Nr. 12 definiert den Begriff als, „Verletzung des Schutzes personenbezogener Daten“, eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.[249]

Der Begriff der Sicherheit ist in der Verordnung nicht definiert. Allerdings regelt Art. 32 die Sicherheit der Verarbeitung. Aus diesem systematischen Zusammenhang lässt sich entnehmen, dass eine Datenschutzverletzung die Verletzung „technischer oder organisatorischer Maßnahmen des Verantwortlichen oder Auftragsverarbeiters meint. [250]

Nach dem Wortlaut kommt es nicht darauf an, ob die Verletzung „unbeabsichtigt oder unrechtmäßig“ geschieht. Ein Verschulden ist also nicht maßgeblich, sodass auch der zufällige oder durch höhere Gewalt ausgelöste Verlust von personenbezogenen Daten zu melden ist. Dies entspricht auch dem Schutzzweck der Definition, die im Zusammenhang mit den Melde- und Benachrichtigungspflichten nach Art. 33 und 34 zu einer Vermeidung von Risiken für die Betroffenen führen soll.[251]

Nach der Definition muss die Sicherheitsverletzung ferner zu einer Kompromittierung der personenbezogenen Daten geführt haben. Und zwar entweder zur „Vernichtung, zum Verlust, zur Veränderung“ oder „zur unbefugten Offenlegung von beziehungsweise unbefugtem Zugang zu personenbezogenen Daten.[252]

Die personenbezogenen Daten sind „vernichtet“, wenn sie unwiederbringlich gelöscht sind. Gemäß Art. 31 Abs. 1 i. V. m. Art. 4 Abs. 9 DS-GVO liegt eine Schutzverletzung bei einer Vernichtung von personenbezogenen Daten vor. Die Vernichtung im

---

249 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 12 DSGVO.

250 *Assion,* Kommentar Datenschutz-Grundverordnung, S.127, Rn.11, a) Verletzung der Sicherheit.

251 *Assion,* Kommentar Datenschutz-Grundverordnung, S.128, Rn.12, b) Unbeabsichtigt oder unrechtmäßig.

252 *Assion,* Kommentar Datenschutz-Grundverordnung, S.128, RN13, c) Vernichtung.

datenschutzrechtlichen Kontext umfasst alle Formen der Datenlöschung nach der DS-GVO, welche die Daten unwiederbringlich machen.[253]

Ausgangspunkt der Definition ist eine Verletzung der Sicherheit. Die Begriffsbestimmung nimmt insoweit Bezug aus Art. 32 DS-GVO, welcher datenverarbeitende Stellen dazu verpflichtet, geeignete technische und organisatorische Datensicherheitsmaßnahmen zu ergreifen. Art. 32 Abs. 2 DS-GVO greift insoweit den Wortlaut von Art. 4 Nr. 12 DS-GVO auf und statuiert, dass hierbei insbesondere solche Risiken zu berücksichtigen sind, die infolge von „[…] Vernichtung, Verlust, Veränderung oder unbefugte[r] Offenlegung von beziehungswese unbefugten Zugang zu personenbezogenen Daten […]“ entstehen können.[254]

Eine Datenschutzverletzung ist nur relevant, wenn sie personenbezogene Daten betrifft. Ein reiner Zugriff auf technische Daten, die keinen Bezug zu einer natürlichen Person zulassen, stellt keine Verletzung dar. Art. 4 Nr. 12 legt ebenfalls fest, dass personenbezogene Daten, die das Schutzobjekt der Norm sind, in irgendeiner Form verarbeitet wurden. Der Begriff der Verarbeitung ist in Art. 4 Nr. 2 definiert und sehr weit gefasst. Dementsprechend kommt dem Merkmal „übermittelt, gespeichert oder sonst verarbeitet“ kaum einschränkende Wirkung zu.[255]

253 *Marshall, Kevin*, Rechtsverträgliche Gestaltung, in Datenschutz und Datensicherheit - DuD, 183.
254 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Seite.180, Rn.299.
255 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 4810 von 87533, Rn.182.

2.14 Art. 4 Nr. 13 DS-GVO genetische Daten

Genetische Daten sind nach Art. 4 Nr. 13 personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen werden.[256]

Genetische Daten können insbesondere im Forschungs- und Medizinbereich verwendet werden, so z.B., um im Rahmen der personalisierten Medizin individuell auf den Patienten abgestimmten Behandlungsmethoden und Therapien zu ermitteln und einzusetzen die eine höhere Erfolgsrate versprechen als „allgemeine" Behandlungen und Therapien.[257]

Genetische Daten sind besonders sensitiv, da sie eine eindeutige Identifizierung ermöglichen und zudem auch Informationen über weitere natürliche Personen, die mit der betroffenen Person verwandt sind, liefern können.[258]

2.15 Art. 4 Nr. 14 DS-GVO biometrische Daten

Biometrische Daten sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den psychischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglicht oder bestätigen. Dazu zählen Gesichtsbilder oder daktyloskopische Daten.[259]

Die Daten - nicht die Merkmale – müssen mit „speziellen technischen Verfahren" gewonnen werden. Die Abgrenzung zu anderweitig gewonnen Daten fällt nicht immer leicht: „Normale Lichtbilder" sollen keine biometrischen Daten sein. Obwohl Lichtbilder mittels Technik erstellt werden, soll es insoweit an einem „speziellen technischen Verfahren" fehlen. (dazu im folgenden **Erwägungsgrund 50**)[260]

---

256 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Seite. 97, Rn.104.
257 *J. Philipp Albrecht,* Datenschutzrecht, Seite.184, Rn.315.
258 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, Seite.299/300, Rn.182.
259 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, S. 98, Rn. 109.
260 *J. Philipp Albrecht,* Datenschutzrecht, S. 342, Rn. 8.

Erwägungsgrund 50

Die Verarbeitung personenbezogener Daten für andere Zwecke als die, für die die personenbezogenen Daten ursprünglich erhoben wurden, sollte nur zulässig sein, wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. In diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten. Ist die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, so können im Unionsrecht oder im Recht der Mitgliedstaaten die Aufgaben und Zwecke bestimmt und konkretisiert werden, für die eine Weiterverarbeitung als vereinbar und rechtmäßig erachtet wird. Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke sollte als vereinbarer und rechtmäßiger Verarbeitungsvorgang gelten. Die im Unionsrecht oder im Recht der Mitgliedstaaten vorgesehene Rechtsgrundlage für die Verarbeitung personenbezogener Daten kann auch als Rechtsgrundlage für eine Weiterverarbeitung dienen. Um festzustellen, ob ein Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, sollte der Verantwortliche nach Einhaltung aller Anforderungen für die Rechtmäßigkeit der ursprünglichen Verarbeitung unter anderem prüfen, ob ein Zusammenhang zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung besteht, in welchem Kontext die Daten erhoben wurden, insbesondere die vernünftigen Erwartungen der betroffenen Personen, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in Bezug auf die weitere Verwendung dieser Daten, um welche Art von personenbezogenen Daten es sich handelt, welche Folgen die beabsichtigte Weiterverarbeitung für die betroffenen Personen hat und ob sowohl beim ursprünglichen als auch beim beabsichtigten Weiterverarbeitungsvorgang geeignete Garantien bestehen.

Hat die betroffene Person ihre Einwilligung erteilt oder beruht die Verarbeitung auf Unionsrecht oder dem Recht der Mitgliedstaaten, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses darstellt, so sollte der Verantwortliche die personenbezogenen Daten ungeachtet der Vereinbarkeit der Zwecke weiterverarbeiten dürfen. In jedem Fall sollte gewährleistet sein, dass die in dieser

Verordnung niedergelegten Grundsätze angewandt werden und insbesondere die betroffene Person über diese anderen Zwecke und über ihre Rechte einschließlich des Widerspruchsrechts unterrichtet wird. Der Hinweis des Verantwortlichen auf mögliche Straftaten oder Bedrohungen der öffentlichen Sicherheit und die Übermittlung der maßgeblichen personenbezogenen Daten in Einzelfällen oder in mehreren Fällen, die im Zusammenhang mit derselben Straftat oder derselben Bedrohung der öffentlichen Sicherheit stehen, an eine zuständige Behörde sollten als berechtigtes Interesse des Verantwortlichen gelten. Eine derartige Übermittlung personenbezogener Daten im berechtigten Interesse des Verantwortlichen oder deren Weiterverarbeitung sollte jedoch unzulässig sein, wenn die Verarbeitung mit einer rechtlichen, beruflichen oder sonstigen verbindlichen Pflicht zur Geheimhaltung unvereinbar ist.[261]

Biometrische Daten werden in **Erwägungsgrund 51** S. 3 insbesondere unter dem Gesichtspunkt von Lichtbildern aufgegriffen. Danach soll die Verarbeitung von Lichtbildern grundsätzlich nicht den Voraussetzungen der Verarbeitung nach Art. 9 unterfallen. Vielmehr sind diese lediglich dann als biometrische Daten und damit als besondere Kategorie personenbezogener Daten einzustufen, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen. Faktisch erfüllt die weit überwiegende Mehrzahl der Aufnahmen von Smartphones, Dash- und Bodycams und Videokameras diese Voraussetzungen.[262]

Allerdings ist zu beachten, dass die Aussage, dass eine „eindeutige Identifizierung" ermöglicht oder bestätigt wurde, nicht statistisch gemeint ist. Bestimmte biometrische Daten mögen eben nicht unter allen Menschen eindeutig sein, solche aber vom Begriff erfasst werden. Es ist (auch angesichts der hohen Zahl lebender Menschen) nicht auszuschließen, dass auch in Bezug auf manche biometrischen Daten zuweilen Identität bei zwei oder mehr Menschen besteht. Gleichwohl hat auch der EuGH festgestellt, dass Fingerabdrücke „objektiv unverwechselbare Informationen über natürliche Personen

261 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 50.

262 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 4884 von 87533, Rn. 196.

enthalten und deren genaue Identifizierung ermöglichen“[263]. Gemeint sind alle stabilen morphologische Merkmale, die körperlich fixiert und grundsätzlich unveränderlich sind (auch Ohrläppchen) in Abgrenzung zu bewegungsorientierten Merkmalen wie Gangart oder Fußstellung.[264]

Erwägungsgrund 51

Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können. Diese personenbezogenen Daten sollten personenbezogene Daten umfassen, aus denen die rassische oder ethnische Herkunft hervorgeht, wobei die Verwendung des Begriffs "rassische Herkunft" in dieser Verordnung nicht bedeutet, dass die Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt. Die Verarbeitung von Lichtbildern sollte nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden, da Lichtbilder nur dann von der Definition des Begriffs "biometrische Daten" erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen. Derartige personenbezogene Daten sollten nicht verarbeitet werden, es sei denn, die Verarbeitung ist in den in dieser Verordnung dargelegten besonderen Fällen zulässig, wobei zu berücksichtigen ist, dass im Recht der Mitgliedstaaten besondere Datenschutzbestimmungen festgelegt sein können, um die Anwendung der Bestimmungen dieser Verordnung anzupassen, damit die Einhaltung einer rechtlichen Verpflichtung oder die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder die Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, möglich ist. Zusätzlich zu den speziellen Anforderungen an eine derartige Verarbeitung sollten die allgemeinen Grundsätze und andere Bestimmungen dieser Verordnung, insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung, gelten. Ausnahmen von dem allgemeinen Verbot der Verarbeitung dieser besonderen Kategorien personenbezogener Daten sollten ausdrücklich vorgesehen

263 Gerichtshof, 17. Oktober 2013 – C-291/12 eur.lex.europa.eu.
264 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Begriffsbestimmungen, S. 53, Rn. 101.

werden, unter anderem bei ausdrücklicher Einwilligung der betroffenen Person oder bei bestimmten Notwendigkeiten, insbesondere wenn die Verarbeitung im Rahmen rechtmäßiger Tätigkeiten bestimmter Vereinigungen oder Stiftungen vorgenommen wird, die sich für die Ausübung von Grundfreiheiten einsetzen.[265]

Eine Besonderheit biometrischer Daten liegt darin, dass sie zwar gelöscht oder verändert werden können, aber Änderungen oder Manipulationen der Datenquelle nicht möglich sind. Insofern weisen biometrische Rohdaten eine enge Verknüpfung zu den genetischen Daten aus Art. 4 Nr. 13 auf. Sie enthalten nicht nur Informationen über die betroffene Person selbst, sondern erlauben auch Verknüpfungen zu anderen Personen und sie ermöglichen so die Generierung weiterer personenbezogener Daten. Darüber hinaus sind biometrische Daten wie genetische Daten besonders anfällig für Diskriminierungen und unterfallen dem besonderen Schutz des Art. 9.[266]

Auch wenn die Nutzung biometrischer Daten stark zugenommen hat, darf nicht übersehen werden, dass biometrische Daten unter die besonderen Kategorien personenbezogener Daten nach Art. 9 fallen und daher eine Verarbeitung dieser Daten grundsätzlich unzulässig ist. Werden also Zugangskontrollen zu Arbeitsstätten oder einem Fitness-Center durch die Nutzung biometrischer Daten durchgeführt (Fingerabdruck-Scanner am Eingang), so wird dies mangels Erforderlichkeit und Verhältnismäßigkeit in der Praxis regelmäßig nur mit Einwilligung zulässig sein. Ohne Einwilligung dürfte auf nicht biometrische Technik auf eine Zugangskarte oder Karte mit Magnetstreifen zurückzugreifen sein.[267]

Der Verwendung biometrischer Fotos kommt im Zuge der verstärkten Nutzung von Social Media-Plattformen eine besondere Bedeutung zu. So werden Fotos per Messenger verschickt oder auf der eigenen Profilseite der Nutzer hochgeladen. Deren Erfassung und Verarbeitung in biometrischen Systemen ist dabei unter anderem an die strengen Voraussetzungen einer Einwilligung geknüpft und stellt Datenverarbeiter insbesondere

265 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 51.

266 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 4998 von 87533, Rn. 204.

267 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 4998 von 87533, Rn. 204.

bei Big Data-Anwendungen hinsichtlich einer klaren Zweckbestimmung vor enorme Herausforderungen.[268]

Biometrische Daten werden auch bei der Videoüberwachung relevant. Sie findet zunehmend durch biometrische Systeme statt. Dabei werden zunehmend auch Gesichtserkennungen durchgeführt sowie zusätzliche Elemente – etwa die Gangart oder Gestik – erfasst.[269]

2.16 Art. 4 Nr. 15 DS-GVO Gesundheitsdaten

„Gesundheitsdaten" personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.[270]

Zu den Gesundheitsdaten zählen nach ErwGr. 35 beispielsweise Informationen zu Krankheiten, Behinderungen, klinische Behandlungen, physiologischem oder biometrischem Zustand einer natürlichen Person sowie Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben abgeleitet wurden. Gesundheitsdaten können daher zugleich genetische und /oder biometrische Daten sein.[271]

Hinsichtlich der Datenherkunft geht die DS-GVO ganz offenkundig davon aus, dass Gesundheitsdaten überwiegend im Rahmen von Gesundheitsdienstleistungen hervorgebracht werden. Als mögliche Datenquelle nennt Erwägungsgrund 35 Ärzte, sonstige Angehörige eines Gesundheitsberufs, Krankenhäuser, Medizinprodukte und In-Vitro-Diagnostika.

---

268 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 4998 von 87533, Rn. 204.

269 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 4998 von 87533, Rn.204.

270 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 15 DSGVO.

271 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, S. 99, Rn. 114.

Erwägungsgrund 35:

Zu den personenbezogenen Gesundheitsdaten sollten alle Daten zählen, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen. Dazu gehören auch Informationen über die natürliche Person, die im Zuge der Anmeldung für sowie der Erbringung von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates für die natürliche Person erhoben werden, Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben, abgeleitet wurden, und Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-Vitro-Diagnostikum stammen.[272]

272 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 35.

2.17 Art. 4 Nr. 16 DS-GVO Hauptniederlassung

Die Datenschutz-Grundverordnung definiert in Art. 4 Nr. 16 eine Hauptniederlassung anhand nachfolgender Auslegung:

- im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung

- im Falle eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt;[273] [274]
- Zum Begriff der Niederlassung gibt **Erwägungsgrund 2*2*** Auskunft.[275] Der Begriff der Niederlassung folgt damit einer flexiblen kontextbezogenen Betrachtungsweise und erfolgt nicht formalistisch. Insofern befindet sich die Niederlassung eines Unternehmens nicht dort, wo es eingetragen ist. Um festzustellen, ob ein Unternehmen, das für eine Datenverarbeitung verantwortlich ist, über eine Niederlassung verfügt, ist vielmehr der Grad an Beständigkeit der Einrichtung sowie die effektive Ausübung der wirtschaftlichen Tätigkeiten unter Beachtung des besonderen Charakters der Tätigkeit und der in Rede stehenden

273 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 16 DSGVO.

274 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 36.

275 *J. Philipp Albrecht,* Datenschutzrecht, S. 346, Rn. 3, Satz.1.

Dienstleistungen auszulegen. Insofern ist auch eine Datenverarbeitung, die durch eine Niederlassung im Rahmen von Werbemaßnahmen gefördert wird, in diese Abwägung miteinzubeziehen. Eine Niederlassung kann dabei auch unter Umständen in einer effektiven und tatsächlichen Tätigkeit, die nur geringer Natur ist, gesehen werden. Dies gilt etwa dann, wenn die Zweitniederlassung nur in Person eines Vertreters besteht. Diese flexible Betrachtungsweise ist somit einer Prüfung des Begriffs der Hauptniederlassung voranzustellen. Hat der Verantwortliche oder der Auftragsverarbeiter indes nur eine Niederlassung in der Union, stellt sich die Frage nach einer bestehenden Hauptniederlassung nicht.[276]

- **Erwägungsgrund 150 Satz 3** statuiert, dass im Rahmen von Art. 83 DS-GVO ein im Verhältnis zu Art. 4 Nr. 18 DS-GVO erweiterter Unternehmensbegriff gelten soll. Art. 83 Abs. 4 - 6 DS-GVO bestimmt insoweit, dass bei der Bußgeldbemessung gegenüber Unternehmen auch deren weltweiter Jahresumsatz als Bemessungsgrundlage (neben der gedeckelten Maximalhöhe von 10 bzw. 20 Mio. Eur.) herangezogen werden kann.[277]

- Der Begriff des Unternehmens soll in diesem Fall kartellrechtlich im Sinne des Art. 101 und Art. 102 AEUV verstanden werden. Insofern steht nicht ein formales, sondern vielmehr ein wettbewerbsrechtlich funktionales Begriffsverständnis im Vordergrund. [278]

- Nach Art. 4 Nr. 16 lit. b ist die Hauptniederlassung des Auftragsverarbeiters bei mehreren Niederlassungen ebenfalls der Ort der Hauptverwaltung. Insofern ist aber zu beachten, dass die Bestimmung der Hauptniederlassung des Auftragsverarbeiters nicht nach den Kriterien gemäß Art. 4 Nr. 16 lit. a erfolgen kann, weil der Auftragsverarbeiter in diesem Sinne grundsätzlich keine Grundsatzentscheidungen trifft. Andernfalls wäre er Verantwortlicher. Folglich ist der Schwerpunkt der wesentlichen Verarbeitungstätigkeiten entscheidend.

---

276 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 5101 von 87533, Rn. 220.
277 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, S. 196, Rn. 369.
278 *J. Philipp Albrecht,* Datenschutzrecht, S. 197, Rn. 370.

Insofern ist daher auch eine flexible und kontextbezogene Betrachtungsweise ausschlaggebend, so dass sich der Prüfungskatalog des Art. 4 Nr. 16 lit. a im Wesentlichen im Rahmen der Feststellung der Hauptniederlassung des Auftragsverarbeiters wiederholt. Dies ergibt sich bereits aus **Erwägungsgrund 36** S. 5.[279]

Erwägungsgrund 22

Jede Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union sollte gemäß dieser Verordnung erfolgen, gleich, ob die Verarbeitung in oder außerhalb der Union stattfindet. Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei nicht ausschlaggebend.[280]

279 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 5212 von 87533, Rn. 228.

280 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 22.

2.18 Art. 4 Nr. 17 DS-GVO Vertreter

Als Vertreter wird eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt, bezeichnet.[281]

Der Vertreter findet zudem in weiteren Regelungen der DS-GVO Erwähnung. Zum einen wird er vereinzelt mit eigenen, originären gesetzlichen Pflichten versehen. So hat er gemäß Art. 30 Abs. 1 DS-GVO das Verarbeitungsverzeichnis zu führen und soll nach Art. 31 DS-GVO mit den zuständigen Aufsichtsbehörden hinsichtlich solcher Maßnahmen zusammenarbeiten, die die Einhaltung der Regelungen der DS-GVO sicherstellen.[282]

Bei Verstößen des Verantwortlichen oder des Auftragsverarbeiters wird der Vertreter Durchsetzungsmaßnahmen unterworfen. Diese Regelung ist deshalb in der Praxis wichtig, weil ein Verantwortlicher oder ein Auftragsverarbeiter, der keine Niederlassung in einem Mitgliedstaat hat, nicht den Durchsetzungsmaßnahmen der Union unterliegt. Insofern wird die Rechtsdurchsetzung erleichtert bzw. ermöglicht.

Art. 4 Nr. 17 stellt eine abschließende Regelung dar. Für nationale Regelungen und Umsetzungsmaßnahmen bleibt daher kein Raum.[283]

Die Bestellung des Vertreters hat nach Art. 4 Nr. 17 DS-GVO i.V. Art. 27 Abs. 1 DS-GVO und **Erwägungsgrund 80** schriftlich und ausdrücklich zu erfolgen; die rein faktische Übernahme der Vertretung genügt daher nicht.[284]

---

281 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art.4 Nr.17 DSGVO.

282 *J. Philipp Albrecht,* Datenschutzrecht, Seite.194, Rn.360.

283 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, 5269 von 87533, Rn.242.

284 *J. Philipp Albrecht,* Datenschutzrecht, S.195, Rn.363.

Erwägungsgrund 80

Jeder Verantwortliche oder Auftragsverarbeiter ohne Niederlassung in der Union, dessen Verarbeitungstätigkeiten sich auf betroffene Personen beziehen, die sich in der Union aufhalten, und dazu dienen, diesen Personen in der Union Waren oder Dienstleistungen anzubieten - unabhängig davon, ob von der betroffenen Person eine Zahlung verlangt wird - oder deren Verhalten, soweit dieses innerhalb der Union erfolgt, zu beobachten, sollte einen Vertreter benennen müssen, es sei denn, die Verarbeitung erfolgt gelegentlich, schließt nicht die umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten oder die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten ein und bringt unter Berücksichtigung ihrer Art, ihrer Umstände, ihres Umfangs und ihrer Zwecke wahrscheinlich kein Risiko für die Rechte und Freiheiten natürlicher Personen mit sich oder bei dem Verantwortlichen handelt es sich um eine Behörde oder öffentliche Stelle. Der Vertreter sollte im Namen des Verantwortlichen oder des Auftragsverarbeiters tätig werden und den Aufsichtsbehörden als Anlaufstelle dienen. Der Verantwortliche oder der Auftragsverarbeiter sollte den Vertreter ausdrücklich bestellen und schriftlich beauftragen, in Bezug auf die ihm nach dieser Verordnung obliegenden Verpflichtungen an seiner Stelle zu handeln. Die Benennung eines solchen Vertreters berührt nicht die Verantwortung oder Haftung des Verantwortlichen oder des Auftragsverarbeiters nach Maßgabe dieser Verordnung. Ein solcher Vertreter sollte seine Aufgaben entsprechend dem Mandat des Verantwortlichen oder Auftragsverarbeiters ausführen und insbesondere mit den zuständigen Aufsichtsbehörden in Bezug auf Maßnahmen, die die Einhaltung dieser Verordnung sicherstellen sollen, zusammenarbeiten. Bei Verstößen des Verantwortlichen oder Auftragsverarbeiters sollte der bestellte Vertreter Durchsetzungsverfahren unterworfen werden.[285]

285 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 80.

2.19 Art. 4 Nr. 18 DS-GVO Unternehmen

„Unternehmen“ bezeichnet eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen.[286]

Art. 4 Nr. 19 definiert die Unternehmensgruppe als eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht. In einer Unternehmensgruppe besteht danach ein Über-Unterordnungsverhältnis.

Nach **Erwägungsgrund 37** sollte das herrschende Unternehmen dasjenige sein, das zum Beispiel aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann. Ein Unternehmen, das die Verarbeitung personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert, sollte zusammen mit diesen als eine „Unternehmensgruppe“ betrachtet werden. Das macht deutlich, dass es bei der Unternehmensgruppe nicht ausschließlich auf eine Beherrschung im gesellschaftsrechtlichen Sinne ankommt, sondern auch faktische Unternehmensgruppen, bei denen z.B. aufgrund von Verträgen bestimmten Unternehmen die Möglichkeit zum Richtlinienerlass gegeben ist, hierunter fallen können.[287]

Erwägungsgrund 37

Eine Unternehmensgruppe sollte aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen bestehen, wobei das herrschende Unternehmen dasjenige sein sollte, das zum Beispiel aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann. Ein Unternehmen, das die Verarbeitung

286 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 18 DSGVO.

287 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 5321 von 87533, Rn.248/249.

personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert, sollte zusammen mit diesen als eine "Unternehmensgruppe" betrachtet werden.[288]

2.20 Art. 4 Nr. 19 DS-GVO Unternehmensgruppe

Als „Unternehmensgruppe“ wird nach Art. 4 Nr. 19 DS-GVO eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht, bezeichnet.“[289]

In einer Unternehmensgruppe besteht danach ein Über-Unterordnungsverhältnis. Nach Erwägungsgrund 37 sollte das herrschende Unternehmen dasjenige sein, das zum Beispiel aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann. Ein Unternehmen, das die Verarbeitung personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert, sollte zusammen mit diesen als eine „Unternehmensgruppe“ betrachtet werden. Das macht deutlich, dass es bei der Unternehmensgruppe nicht ausschließlich auf eine Beherrschung im gesellschaftsrechtlichen Sinne ankommt, sondern auch faktische Unternehmensgruppen, bei denen z.B. aufgrund von Verträgen bestimmten Unternehmen die Möglichkeit zum Richtlinienerlass gegeben ist, hierunter fallen können.[290]

Die Unternehmensgruppe ist an verschiedenen Stellen der DS-GVO von Bedeutung. Insbesondere im Zusammenhang mit der Möglichkeit, auf Grundlage von verbindlichen internen Datenschutzvorschriften (**B**inding **C**orporate **R**ules – **BCR**) personenbezogene Daten in Drittländer zu übermitteln. Erwägungsgrund 48 nennt die Unternehmensgruppe als besonderes Beispiel dafür, dass die verantwortlichen Stellen in einer Unternehmensgruppe ein besonderes berechtigtes Interesse an einer Übermittlung von

---

288 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 37.

289 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art.4 Nr.19 DSGVO.

290 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 5321 von 87533, Rn. 249.

Daten innerhalb der Unternehmensgruppe haben können. Nach Art. 37 Abs. 2 darf eine Unternehmensgruppe einen gemeinsamen betrieblichen Datenschutzbeauftragten bestellen, sofern der Datenschutzbeauftragte von jeder Niederlassung leicht erreicht werden kann. Art. 88 Abs. 2 verlangt, dass Mitgliedstaaten, die von der Ausnahme des Art. 88 Abs. 1 Gebrauch machen und gesonderte Regelungen zum Umgang mit Beschäftigtendaten erlassen, besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person vorsehen.[291]

2.21 Art. 4 Nr. 20 DS-GVO verbindliche interne Datenschutzvorschrift

„Verbindliche interne Datenschutzvorschriften“ bezeichnen Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern.[292]

Eine detaillierte Regelung zu den verbindlichen internen Datenschutzvorschriften findet sich in Art. 47 der DS-GVO. Darüber hinaus nimmt Art. 4 Nr. 20 Bezug auf die Niederlassung eines Verantwortlichen oder Auftragsverarbeiters. Insofern sind die inhaltlichen Bezüge zu Art. 4 Nr. 7, 8 und 16 zu beachten. Ferner ist hinsichtlich des Begriffs des Unternehmens und der Unternehmensgruppe in Art. 4 Nr. 20 auf Art. 4 Nr. 18 und 19 zu verweisen. Diese internen Datenschutzvorschriften stellen letztlich Regelungen zum Schutz personenbezogener Daten im Hinblick auf Datenübermittlungen in Drittländer dar, zu deren Einhaltung sich ein in der EU niedergelassener Verantwortlicher oder Auftragsdatenverarbeiter verpflichtet. Insofern erlauben diese internen Regelungen dem Verantwortlichen oder Auftragsverarbeiter personenbezogene

291 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 5367 von 87533, Rn. 251 - 254.

292 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 20 DSGVO.

Daten auch dann an ein verbundenes Unternehmen in einem Drittland zu übermitteln, wenn dieses nicht über ein der DS-GVO entsprechendes Datenschutzniveau verfügt. Die verbundenen Unternehmen werden so zu Maßnahmen zum Schutz personenbezogener Daten verpflichtet. Folglich können interne Datenschutzvorschriften als geeignete Garantien nach Art. 46 Abs. 1 Datenübermittlungen in Drittländer ohne ein der DS-GVO entsprechendes angemessenes Datenschutzniveau rechtfertigen, wenn die Voraussetzungen des Art. 47 Abs. 1 und 2 vorliegen. Dazu müssen die Datenschutzvorschriften insbesondere rechtlich bindend sein und die inhaltlichen Anforderungen des Kataloges des Art. 47 Abs. 2 erfüllen.[293]

2.22 Art. 4 Nr. 21 DS-GVO Aufsichtsbehörde

Als „Aufsichtsbehörde“ wird eine von einem Mitgliedstaat gemäß Artikel 51 eingerichtete unabhängige staatliche Stelle, bezeichnet.[294]

Jeder Mitgliedstaat sieht nach Art. 51 Abs. 1 vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird. Die Existenz einer unabhängigen Datenschutzaufsicht wird bereits durch das primäre Unionsrecht vorgegeben.[295]

293 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 5367 von 87533, Rn.255-259.

294 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 21 DSGVO.

295 *J. Philipp Albrecht,* Datenschutzrecht, S. 352, Rn. 1.

2.23 Art. 4 Nr. 22 DS-GVO betroffene Aufsichtsbehörde

Ob eine Aufsichtsbehörde nach Art. 4 Nr. 22 DS-GVO **betroffen** ist, hängt von den nachfolgenden Kriterien ab. Diese lauten wie folgt:

- Unter der Voraussetzung, dass der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist,
- Sofern diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder
- Für den Fall, dass eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde;[296]

Der Begriff der „betroffenen Aufsichtsbehörde“ wurde im Gesetzgebungsverfahren durch den Rat im Zuge der Überarbeitung des Verfahrens der Zusammenarbeit und Kohärenz (hierzu Art. 60 ff.) eingeführt und im Laufe des Weiteren Verfahrens nicht mehr geändert.[297]

Für die Qualifizierung als betroffene Aufsichtsbehörde gibt es nach Nr. 22 drei mögliche alternative Anknüpfungspunkte. Lit. a. setzt am territorialen Bezug zum Datenverarbeiter durch dessen Niederlassung an, lit. b am territorialen Bezug zu Betroffenen und lit. c an dem territorialen Bezug einer konkreten Abwehrmaßnahme des Betroffenen nämlich einer Beschwerde.[298]

Der Begriff der Niederlassung wird dabei in der Rechtsprechung des EuGHs weit ausgelegt. Sie setzt die effektive und tatsächliche Ausübung einer wirtschaftlichen Tätigkeit mittels einer festen Einrichtung voraus, wobei die Rechtsform unerheblich ist. **Erwägungsgrund 22** S. 2 und 3 übernehmen diese Wertung. Um festzustellen, ob ein Unternehmen, das für eine Datenverarbeitung verantwortlich ist, über eine Niederlassung verfügt, ist vielmehr der Grad an Beständigkeit der Einrichtung sowie die effektive Ausübung der wirtschaftlichen Tätigkeiten unter Beachtung des besonderen Charakters

296 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 22 DSGVO.
297 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, S. 179, Rn. 1.
298 *J. Philipp Albrecht,* Datenschutzrecht, S. 353, Rn. 4.

der Tätigkeit und der in Rede stehenden Dienstleistungen auszulegen. Eine Niederlassung kann dabei auch unter Umständen in einer effektiven und tatsächlichen Tätigkeit, die nur geringer Natur ist, gesehen werden, etwa dann, wenn die Zweitniederlassung nur in Person eines Vertreters besteht. Der Begriff der Niederlassung folgt damit einer flexiblen kontextbezogenen Betrachtungsweise und erfolgt nicht formalistisch.[299]

Art. 4 Nr. 22 lit. b stellt wie Art. 4 Nr. 23 lit. b auf die erheblichen Auswirkungen auf die betroffenen Personen ab. Die Möglichkeit erheblicher Auswirkungen ist ausweislich des Wortlauts der Verordnung („haben kann“) bereits ausreichend. „Auswirkungen“ ist dabei weit gefasst und schließt sowohl rechtliche als auch tatsächliche Auswirkungen mit ein, sofern diese nicht unerheblich sind. Es ist nicht zu verleugnen, dass der Begriff der Auswirkungen kaum Konturen aufweist. Eine Definition der Auswirkungen oder Erheblichkeit enthält Art. 4 Nr. 22 lit. b nicht. Insofern betont **Erwägungsgrund 124** S. 4, dass der Datenschutzausschuss aufgefordert ist, Leitlinien zu den Kriterien auszugeben, die bei der Feststellung zu berücksichtigen sind, ob die fragliche Verarbeitung erhebliche Auswirkungen auf betroffene Personen hat.[300]

Erwägungsgrund 124

Findet die Verarbeitung personenbezogener Daten im Zusammenhang mit der Tätigkeit einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union statt und hat der Verantwortliche oder der Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat oder hat die Verarbeitungstätigkeit im Zusammenhang mit der Tätigkeit einer einzigen Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der Union erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat bzw. wird sie voraussichtlich solche Auswirkungen haben, so sollte die Aufsichtsbehörde für die Hauptniederlassung des Verantwortlichen oder Auftragsverarbeiters oder für die einzige Niederlassung des Verantwortlichen oder Auftragsverarbeiters als federführende Behörde fungieren. Sie sollte mit den anderen Behörden zusammenarbeiten, die betroffen sind, weil der Verantwortliche oder Auftragsverarbeiter eine Niederlassung im Hoheitsgebiet ihres Mitgliedstaats hat, weil

299 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 5476 von 87533, Rn. 272.

300 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 5476 von 87533, Rn. 273 - 274.

die Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz in ihrem Hoheitsgebiet hat oder weil bei ihnen eine Beschwerde eingelegt wurde. Auch wenn eine betroffene Person ohne Wohnsitz in dem betreffenden Mitgliedstaat eine Beschwerde eingelegt hat, sollte die Aufsichtsbehörde, bei der Beschwerde eingelegt wurde, auch eine betroffene Aufsichtsbehörde sein. Der Ausschuss sollte - im Rahmen seiner Aufgaben in Bezug auf die Herausgabe von Leitlinien zu allen Fragen im Zusammenhang mit der Anwendung dieser Verordnung - insbesondere Leitlinien zu den Kriterien ausgeben können, die bei der Feststellung zu berücksichtigen sind, ob die fragliche Verarbeitung erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat und was einen maßgeblichen und begründeten Einspruch darstellt.[301]

Als dritten Anknüpfungspunkt nennt Art. 4 Nr. 22 lit. c, dass eine Beschwerde bei der Aufsichtsbehörde eingereicht wurde. Die Beschwerde steht damit in unmittelbarem Zusammenhang zu Art. 57 Abs. 1 lit. f und Art. 77. Da im Rahmen von Art. 77 das Beschwerderecht sich etwa nach dem Aufenthaltsort, dem Arbeitsplatz oder dem Ort des mutmaßlichen Verstoßes richtet, eröffnet Art. 4 Nr. 22 lit. c weitreichende Möglichkeiten die Stellung einer Aufsichtsbehörde als „betroffene Aufsichtsbehörde“ zu begründen. Dies unterstreicht Erwägungsgrund 141.[302]

Erwägungsgrund 141

Jede betroffene Person sollte das Recht haben, bei einer einzigen Aufsichtsbehörde insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts eine Beschwerde einzureichen und gemäß Artikel 47 der Grundrechtscharta einen wirksamen gerichtlichen Rechtsbehelf einzulegen, wenn sie sich in ihren Rechten gemäß dieser Verordnung verletzt sieht oder wenn die Aufsichtsbehörde auf eine Beschwerde hin nicht tätig wird, eine Beschwerde teilweise oder ganz abweist oder ablehnt oder nicht tätig wird, obwohl dies zum Schutz der Rechte der betroffenen Person notwendig ist. Die auf eine Beschwerde folgende Untersuchung sollte vorbehaltlich gerichtlicher Überprüfung so

301 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 124.

302 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, 5535 von 87533, Rn. 276.

weit gehen, wie dies im Einzelfall angemessen ist. Die Aufsichtsbehörde sollte die betroffene Person innerhalb eines angemessenen Zeitraums über den Fortgang und die Ergebnisse der Beschwerde unterrichten. Sollten weitere Untersuchungen oder die Abstimmung mit einer anderen Aufsichtsbehörde erforderlich sein, sollte die betroffene Person über den Zwischenstand informiert werden. Jede Aufsichtsbehörde sollte Maßnahmen zur Erleichterung der Einreichung von Beschwerden treffen, wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.[303]

303 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 141.

2.24 Art. 4 Nr. 23 DS-GVO grenzüberschreitende Verarbeitung

Unter grenzüberschreitender Verarbeitung ist, eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat erfolgt, zu verstehen. Darüber hinaus, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann. Zu beachten ist, dass sich der Begriff, **grenzüberschreitende Verarbeitung** auf die Verarbeitung, die Übermittlung und Verbreitung von Daten innerhalb des EU-Binnenmarktes bezieht. Drittstaaten werden in Art. 44 DS-GVO behandelt.

Eine grenzüberschreitende Verarbeitung liegt vor, wenn die Verarbeitung im Rahmen von Niederlassungen des Verantwortlichen oder Auftragsverarbeiters in mehr als in einem Mitgliedstaat stattfindet, oder auch wenn die Verarbeitung zwar nur im Rahmen einer einzelnen Niederlassung stattfindet, aber erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstatt hat.[304] [305]

In unterschiedlichen Mitgliedstaaten müssen personenbezogene Daten verarbeitet werden. Eine bloße Übermittlung personenbezogener Daten zwischen zwei Verantwortlichen in unterschiedlichen Mitgliedstaaten ist daher noch nicht ausreichend, um die grenzüberschreitende Relevanz (vgl. Erwägungsgrund 138 S. 2) einer Verarbeitung zu begründen. Eine grenzüberschreitende Verarbeitung liegt dagegen vor, wenn ein Auftragsverarbeiter in einem Mitgliedstat personenbezogene Daten eines Verantwortlichen aus einem anderen Mitgliedstaat nutzt, da die Verarbeitung durch

304 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, S. 253, Rn. 66.

305 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 23 DSGVO.

Verantwortlichen und Auftragsverarbeiter als eine Einheit angesehen wird und damit grenzüberschreitend ist.[306] [307]

Art. 4 Nr. 23 lit. b knüpft an die erheblichen Auswirkungen bei dem oder den Betroffenen an. Da Datenverarbeitungen, die lediglich im Rahmen der Tätigkeit einer einzelnen Niederlassung stattfinden, nicht als grenzüberschreitend anzusehen sind, gilt dies abweichend von diesem Grundsatz nach Art. 4 Nr. 23 lit. b dann nicht, wenn die Datenverarbeitung erhebliche Auswirkungen auf die betroffenen Personen haben kann. Insofern ist die Möglichkeit erheblicher Auswirkungen ausweislich des Wortlauts der Verordnung bereits ausreichend.[308]

Erwägungsgrund 138

Die Anwendung dieses Verfahrens sollte in den Fällen, in denen sie verbindlich vorgeschrieben ist, eine Bedingung für die Rechtmäßigkeit einer Maßnahme einer Aufsichtsbehörde sein, die rechtliche Wirkungen entfalten soll. In anderen Fällen von grenzüberschreitender Relevanz sollte das Verfahren der Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden zur Anwendung gelangen, und die betroffenen Aufsichtsbehörden können auf bilateraler oder multilateraler Ebene Amtshilfe leisten und gemeinsame Maßnahmen durchführen, ohne auf das Kohärenzverfahren zurückzugreifen.[309]

306 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, S. 106, Rn. 150, lit. a.

307 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 138.

308 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 5599 von 87533, Rn. 288.

309 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 138.

2.25 Art. 4 Nr. 24 DS-GVO maßgeblicher und begründeter Einspruch

Einen Einspruch im Hinblick darauf, ob ein Verstoß gegen diese Verordnung vorliegt oder nicht oder ob die beabsichtigte Maßnahme gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung steht, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen.[310]

Die Legaldefinition des maßgeblichen und begründeten Einspruchs ist wesentlich für das in Art. 60 Abs. 4 und 6 geregelte Verfahren der Zusammenarbeit zwischenfederführender Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden sowie für das Streitbeilegungsverfahren vor dem Europäischen Datenschutzausschuss nach Art. 65 Abs. 1 lit. a. Das Wort „maßgeblich“, dass in der veröffentlichen Fassung der Verordnung an die Stelle des Wortes „relevant“ getreten ist, hat nach systematischer Auslegung keine eigenständige formelle Bedeutung gegenüber dem materiellen Begriff „begründet“.[311]

Beide Begriffe werden auch an anderer Stelle vergleiche hierzu Art. 60 Abs. 4) synchron verwendet. Nur ein begründeter Einspruch kann maßgeblich sein.[312] Ein Einspruch kann sich stets nur gegen einen Beschlussentwurf der federführenden Behörde richten.[313]

Ein Einspruch ist nur dann maßgeblich und begründet, wenn mit ihm geltend gemacht wird, dass die federführende Aufsichtsbehörde in ihrem Beschlussentwurf zu Unrecht von einem bzw. keinem Verstoß des Verantwortlichen oder des Auftragsverarbeiters gegen die DS-GVO ausgegangen ist. Der Einspruch kann ausweislich des Wortlauts auch damit begründet werden, ob die beabsichtigte Maßnahme gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit der DS-GVO steht. In beiden Alternativen muss der Einspruch den formalen Anforderungen nach Art. 4 Nr. 23 Hs. 2 genügen: So muss sich aus ihm die Tragweite der Risiken ergeben, die von dem Beschlussentwurf für die Grundrechte und Grundfreiheiten der betroffenen Personen oder für den freien

310 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 24 DSGVO.
311 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, Seite. 184, Rn.1.
312 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, Seite. 184, Rn.1.
313 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, Seite. 184, Rn.1.

Verkehr von personenbezogenen Daten in der Union ausgehen. Dabei bezeichnet „begründet“ lediglich, dass die einspruchsführende Behörde ihre Bedenken im Sinne der o.g. Tatbestandsalternativen vortragen muss. Der Verstoß muss aber nicht tatsächlich gegeben sein. Dies folgt bereits daraus, dass der Wortlaut auf die Tragweite der Risiken und nicht auf den Verstoß als solchen abstellt.[314]

Nach **Erwägungsgrund 124** soll der Europäische Datenschutzausschuss Leitlinien zu den Kriterien ausgeben können, die bei der Feststellung zu berücksichtigen sind, was einen maßgeblichen und begründeten Einspruch darstellt.[315]

Erwägungsgrund 124:

Findet die Verarbeitung personenbezogener Daten im Zusammenhang mit der Tätigkeit einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union statt und hat der Verantwortliche oder der Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat oder hat die Verarbeitungstätigkeit im Zusammenhang mit der Tätigkeit einer einzigen Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der Union erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat bzw. wird sie voraussichtlich solche Auswirkungen haben, so sollte die Aufsichtsbehörde für die Hauptniederlassung des Verantwortlichen oder Auftragsverarbeiters oder für die einzige Niederlassung des Verantwortlichen oder Auftragsverarbeiters als federführende Behörde fungieren. Sie sollte mit den anderen Behörden zusammenarbeiten, die betroffen sind, weil der Verantwortliche oder Auftragsverarbeiter eine Niederlassung im Hoheitsgebiet ihres Mitgliedstaats hat, weil die Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz in ihrem Hoheitsgebiet hat oder weil bei ihnen eine Beschwerde eingelegt wurde. Auch wenn eine betroffene Person ohne Wohnsitz in dem betreffenden Mitgliedstaat eine Beschwerde eingelegt hat, sollte die Aufsichtsbehörde, bei der Beschwerde eingelegt wurde, auch eine betroffene Aufsichtsbehörde sein. Der Ausschuss sollte — im Rahmen seiner Aufgaben in Bezug auf die Herausgabe von Leitlinien zu allen Fragen im Zusammenhang mit der Anwendung dieser Verordnung — insbesondere Leitlinien zu den Kriterien ausgeben können, die bei der Feststellung zu berücksichtigen sind, ob die

314 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, 5657 von 87533, Rn. 292.

315 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, Seite. 315, Rn. 265.

fragliche Verarbeitung erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat und was einen maßgeblichen und begründeten Einspruch darstellt.[316]

2.26 Art. 4 Nr. 25 DS-GVO Dienst der Informationsgesellschaft

Unter Dienst der Informationsgesellschaft, ist eine Dienstleistung im Sinne des Art. 1 Nr. 1 lit. b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates, zu verstehen.[317] Die Definition in Art. 1 Nr. 1 lit. b der RL 2015/1535 lautet wie folgt: „jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung". Im Sinne dieser Definition bezeichnet der Ausdruck

- „im Fernabsatz erbrachte Dienstleistung" eine Dienstleistung die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht wird.
- „elektronisch erbrachte Dienstleistung" eine Dienstleistung, die mittels Geräte für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird;
- „auf individuellen Abruf eines Empfängers erbrachte Dienstleistung" eine Dienstleistung die durch die Übertragung von Daten auf individuelle Anforderung erbracht wird.[318]

Folglich sind nach S. 1 jener Definition fünf Voraussetzungen kumulativ zu erfüllen. Das Angebot muss eine (1) i.d.R. gegen Entgelt, (2) elektronisch, (3) im Fernabsatz, (4) auf individuellem Abruf eines Empfängers erbrachte (5) Dienstleistung darstellen. Die

316 Amtsblatt der Europäischen Union 04.05.2016 (Erwägungsgrund 124:).
317 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 25 DSGVO.
318 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, S. 186, Rn. 4.

Voraussetzungen (2), (3) und (4) des elektronischen Fernabsatzes und des individuellen Abrufs werden in S. 2 lit. i bis lit. iii jener Definition bereits näher und positiv geklärt.[319]

Der Begriff der **Dienstleistung** bezieht sich auf Art. 56 AEUV. Die umfangreiche Rechtsprechung des EuGHs zu diesem Begriff stellt unter anderem klar, dass die Bedingung des Erbringens der Dienstleistung in der Regel gegen Entgelt nicht verlangt, dass im konkreten Fall der Nutzer der Dienstleistung eine finanzielle Gegenleistung erbringt. Insbesondere – aber nicht nur- ist hier an Dienste zu denken, die dem Nutzer ohne finanzielle Gegenleistung angeboten werden und die personenbezogenen Daten als Gegenleistung nutzen. Im Fernabsatz erbracht ist eine Dienstleistung, wenn sie bei nicht gleichzeitiger körperlicher Anwesenheit der Beteiligten unter Einsatz eines Kommunikationsmittels erbracht wird, wobei es auf den Übertragungsweg nicht ankommt. Die Dienstleistung muss elektronisch erbracht werden, wie es typischerweise bei Onlineangeboten der Fall ist. Erfasst werden nur Dienstleistungen, die auf individuellen Abruf hin erbracht werden. Lineare Angebote wie Rundfunkangebote folgen einem vorab festgelegten Sendeplan und fallen nicht unter die Dienste der Informationsgesellschaft.[320]

319 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, S. 186, Rn. 5.
320 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 5657 von 87533, Rn.297/298.

2.27 Art. 4 Nr. 26 DS-GVO internationale Organisation

Die internationale Organisation“ ist eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.[321]

Die kurze Erläuterung der Bezeichnungen soll hier nur einen groben Überblick über die Besonderheiten der teilweise neuen Bezeichnungen geben. Jeder einzelne Artikel hat seine Besonderheit und sollte vollumfänglich betrachtet werden.

Warum die Datenschutz-Grundverordnung zu einer Verordnung angehoben wurde, ist unter dem Punkt Rechtsakte der EU angesprochen worden. Was ein erheblicher Diskussionsstoff mit sich brachte war die Anhebung der Bußgelder auf ein nie dagewesenes Niveau.

Art. 4 Nr. 25 definiert den Dienst der Informationsgesellschaft nicht eigenständig, sondern verweist auf die entsprechende Definition in Art. 1 Nr. 1 lit. b der **RL 2015/ 1535**. Dasselbe Begriffsverständnis liegt auch der E-Commerce-Richtlinie zu Grunde. Besondere Berücksichtigung finden die Dienste der Informationsgesellschaft in der DS-GVO bei der Erteilung der Zustimmung zur Verarbeitung, insbesondere solcher Dienste für Kinder gem. Art. 8, sowie beim Recht auf Löschung bzw. Vergessenwerden nach Art. 17.[322]

Die Definition der DS-GVO entspricht im Wesentlichen der im Völkerrecht üblichen Begriffsbestimmung, wonach eine solche Organisation auf einem völkerrechtlichen Vertrag beruht und einen mitgliedschaftlich strukturierten Zusammenschluss von zwei oder mehreren Völkerrechtssubjekten darstellt, der mit eigenen Organen Angelegenheiten von gemeinsamem Interesse besorgt.[323]

---

321 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 26 DSGVO.

322 *Bäcker,* Datenschutz-Grundverordnung, Art. 4, Nr. 26, Rn. 1.

323 *Gola u. a.* (Hrsg.), Datenschutz-Grundverordnung, Gola, Art. 4, Rn. 103 - zzgl. Kommentierung Art. 96 DSGVO.

Erwähnung findet der Begriff der internationalen Organisation auch in Art. 96. Die Norm bestimmt, dass internationale Übereinkünfte, die von den Mitgliedstaaten vor dem Inkrafttreten der DS-GVO zur Übermittlung personenbezogener Daten an Drittländer oder die genannten internationalen Organisationen im Einklang mit dem vor Inkrafttreten der DS-GVO geltenden Unionsrecht abgeschlossen wurden, in Kraft bleiben, bis sie geändert, ersetzt oder gekündigt werden.[324]

2.28 Cookies

Bei Cookies handelt es sich grundsätzlich um Textdateien, welche vom aufgerufenen Server auf dem Rechner des Nutzers angelegt werden. Sie dienen in erster Linie dem Transport von Informationen über mehrere Webseitenaufrufe hinweg und stellen in diesem Umfeld eine etablierte Technik dar.[325] [326]

Gabler definiert Cookies als „eine Datei, die auf einem lokalen Rechner abgelegten Daten einer Webseite, die den Anwender, der an diesem Rechner das World Wide Web nutzt, **eindeutig identifizieren** und Informationen über sein **Surfverhalten speichern** können…“[327]

Der europäische Gesetzgeber hat in seiner Richtlinie aus dem Jahr 2002 (ePrivacy - RL) das Setzen von Cookies an bestimmte Voraussetzungen gekoppelt (vgl. Art. 5 Abs. 3 ePrivacy - RL). Demnach hat der nationale Gesetzgeber Regelungen zu definieren, die Cookies nur das zulassen, wenn der Internetnutzer im Vorfeld **klar und umfassend** über den Einsatz, die Speicherung und den Zweck der Verarbeitung informiert wird.[328] In der Folge stellte sich diese Informationspflicht als **unzureichend** heraus, sodass mit der

---

324 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 5708 von 87533, Rn. 300.

325 *Barth. A*, HTTP State Management Mechanism, Standards Track, Internet Engineering Task Force (IETF), U.C Berkeley April 2011, https://tools.ietf.org/pdf/rfc6265.pdf.

326 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Broy, S. 537, Rn. 11 (Teil B).

327 *Gabler Wirtschaftslexikon*, Cookie, Definition Cookie, Revision von Cookie vom 19.02.2018 06.2020, https://wirtschaftslexikon.gabler.de/definition/cookie-27577/version-251226.

328 RICHTLINIE 2002/58/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) vom 12.07.2002.

Cookie-Richtlinie aus dem Jahr 2009 ein Einwilligungserfordernis in Art. 5 Abs. 3 ePrivacy - RL implementiert wurde.[329]

In der Datenschutz-Grundverordnung werden Cookies lediglich einmal namentlich erwähnt. Spezielle Regelungen zu Cookies und Nutzung von Webseiten enthält die DS-GVO nicht.[330] Hierzu ist der Erwägungsgrund 30 zu betrachten. Dieser führt aus:

Erwägungsgrund 30

Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies **kann** Spuren hinterlassen, die insbesondere in **Kombination** mit **eindeutigen Kennungen** und anderen beim Server eingehenden Informationen dazu benutzt werden können, **um Profile der natürlichen Personen zu erstellen und sie zu identifizieren**.[331]

Diese Definition erfordert in der Folge das Betrachten des Art. 4 Nr. 1 DS-GVO der den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten als Grundlage des Datenschutzes anführt. In diesem Zusammenhang sind ebenfalls die Einwilligung nach Art. 6 Abs. 1 lit. a sowie das Profiling nach Art. 4 Nr. 4 DS-GVO zu betrachten.

Die DS-GVO führt die Grundsätze des sogenannten „Systemdatenschutzes“ fort. Unter der DS-GVO wird der „Datenschutz durch Technikgestaltung (Privacy by Design) und

329 RICHTLINIE 2009/136/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, in: Amtsblatt der Europäischen Union,

330 *Spindler/Schmitz/Liesching,* Telemediengesetz mit Netzwerkdurchsetzungsgesetz; Kommentar, 2. Aufl. 2018, Schmitz, S. 455, Rn. 21 S. 1 TMG.

331 *RICHTLINIE (EU) 2016/ 679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES - vom 27. April 2016*, Erwägungsgründe - VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgründe Datenschutz-Grundverordnung, in Amtsblatt der Europäischen Union 04.05.2016.

durch datenschutzfreundliche Voreinstellung (Privacy by Default)“ in Art. 25 DS-GVO bestimmt.[332]

§ 13 Abs. 1 TMG verlangt, dass der Nutzer zu Beginn des Nutzungsvorgangs über „Art, Umfang und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten“ zu unterrichten ist.[333]

Personenzug ist gegeben, wenn Cookies den Namen oder andere Informationen enthalten, die es ermöglichen, eine Person zu bestimmen.[334] Liegt ein Personenbezug vor, ist § 13 Abs. 1 Satz 1 TMG und nicht § 13 Abs. 1 Satz 2 TMG anwendbar.[335] Der Personenbezug der Cookies ist Anwendungsvoraussetzung für das **TMG** (**T**ele**m**edien**g**esetz) und die Unterrichtungspflicht nach § 13 Abs. 1 Satz 2. Die Frage des Personenbezugs im Sinne des § 3 Abs. 1 BDSG ist nach den allgemein hierfür geltenden Kriterien zu bestimmen. Für die Bestimmbarkeit kommt es deshalb auf die Kenntnisse, Mittel und Möglichkeiten der speichernden Stelle an.[336]

Da Cookies (zunächst) nicht selbst den Rückschluss auf die Identität eines bestimmten Nutzers zulassen, ist der Personenbezug nur möglich, wenn eine Identifizierung über eine Verknüpfung mit anderen personenbezogenen Daten, wie etwa einer IP-Adresse oder einer Zugangskennung möglich. Diesbezüglich ist nach den Urteilen von EuGH und dem darauf basierenden BGH-Urteil nunmehr von einem Personenbezug sowohl bei statischen wie auch bei dynamischen IP-Adressen auszugehen.[337] Da die IP-Adressen beim Setzen und Auslesen von Cookies erhoben werden, liegt in der Folge auch für das Cookie ein Personenzug vor. Es wird deshalb vertreten, dass hierfür die allgemeinen Regeln der DS-GVO zu den Informationspflichten nach Art. 12 – 14 gelten, zumal in Art. 13 Abs. 2 lit. f DS-GVO eine Unterrichtungspflicht im speziellen Fall des „Profiling“ normiert ist.[338]

---

332 *Spindler/Schmitz/Liesching,* Telemediengesetz mit Netzwerkdurchsetzungsgesetz; Kommentar, 2. Aufl. 2018, Schmitz, S. 450, Rn. 4 Abs. 1 TMG.

333 *Spindler/Schmitz/Liesching,* Telemediengesetz mit Netzwerkdurchsetzungsgesetz; Kommentar, 2. Aufl. 2018, Schmitz, S. 451, Rn. 7 S. 1 TMG.

334 BGH - Bundesgerichtshof, 05. Oktober 2017 – I ZR 7/16 Der Bundesgerichtshof (2017).

335 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Schreibauer, S. 2242, Rn. 19, § 13 TMG.

336 *Spindler/Schmitz/Liesching,* Telemediengesetz mit Netzwerkdurchsetzungsgesetz; Kommentar, 2. Aufl. 2018, Schmitz, S. 453, Rn. 13 TMG.

337 *Spindler/Schmitz/Liesching,* Telemediengesetz mit Netzwerkdurchsetzungsgesetz; Kommentar, 2. Aufl. 2018, Schmitz, S. 453, Rn. 13 TMG.

338 *Spindler/Schmitz/Liesching,* Telemediengesetz mit Netzwerkdurchsetzungsgesetz; Kommentar, 2. Aufl. 2018, Schmitz, S. 455, Rn. 21 TMG.

3 Datenschutzrechtliche Grundprinzipien

Die wesentlichen Grundsätze des neuen EU-Datenschutzrechts sind in Art. 5 DS-GVO geregelt. Ein klares Verständnis der in Art. 5 DS-GVO normierten Vorgaben ist für die Auslegung und Anwendung der Vorschriften der gesamten Verordnung notwendig.[339] Die allgemeinen Grundsätze der Datenverarbeitung, die nach Art. 5 der Verordnung gelten, sind allesamt gut bekannt, egal ob es um den **Grundsatz der Transparenz**, der **Zweckbindung**, der **Datensparsamkeit** oder der **Richtigkeit** der Datenverarbeitung geht. Die Vorgabe der Datensparsamkeit – die Verordnung spricht von Datenminimierung – findet sich dann auch noch einmal in Art. 23 in der Gestalt eines technischen Datenschutzes normiert. Die für die Datenverarbeitung Verantwortlichen haben danach die Systeme technisch derart auszugestalten, dass die Risiken für die Rechte und Freiheiten der betroffenen Personen minimiert werden. Des Weiteren haben die Verantwortlichen durch technische Voreinstellungen sicherzustellen, dass tatsächlich nur diejenigen Daten verarbeitet werden, deren Verarbeitung zum Erreichen eines bestimmten Zwecks erforderlich ist. Art. 23 entspricht damit im Wesentlichen dem Konzept der Datenvermeidung und -sparsamkeit, wie es von § 3a BDSG bekannt ist Ein anderer zentraler Grundsatz des deutschen Datenschutzrechts, die Direkterhebung (§ 4 Abs. 2 BDSG), hat hingegen keinen Eingang in die Verordnung gefunden – zumindest nicht ausdrücklich. Art. 14a sieht lediglich eine Reihe von Informationspflichten für den Fall vor, dass Daten nicht bei der betroffenen Person erhoben wurden.[340]

Die datenschutzrechtlichen Grundprinzipien der Rechtmäßigkeit, Transparenz, Zweckbindung, Datensparsamkeit, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit werden aus Art. 8 Abs. 2 DS-GVO abgeleitet und in Art. 5 Abs. 1 DS-GVO aufgeführt.[341] Art. 5 DS-GVO gibt die folgenden Grundsätze vor:

339 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 20, Rn. 62.
340 *DuD* Datenschutz Datensich 2016, 155 (Seite.156, Abs.2.1).
341 AD Legendum AL 1/2018, 1 ((Ad Legendum, AD Legendum 1/2018, S. 16 S. 17, D).

3.1 Rechtmäßigkeit (Verbot mit Erlaubnisvorbehalt), (Art. 5 Abs. 1 lit. a Alt.1 DS-GVO)

Die Verarbeitung personenbezogener Daten muss rechtmäßig sein, Art. 5 Abs.1 lit. a DS-GVO. Nach Art. 6 Abs.1 DS-GVO ist eine Verarbeitung nur dann rechtmäßig, wenn die Voraussetzungen eines der nach der Verordnung zulässigen Erlaubnistatbestände vorliegen. Beispielsweise enthalten Art. 6 und Art. 9 DS-GVO eine **Reihe von Erlaubnistatbeständen**.[342]

Art. 6 DS-GVO:

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
b. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
c. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
d. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
e. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Dies gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommener Verarbeitung. …“ [343] [344]

342 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 21, Rn. 66.
343 *Schneider,* Datenschutz, 2. Aufl. 2019, S. 132, Art. 6 Abs. 1.
344 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 6 DSGVO.

Art. 9 DS-GVO

Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

a. Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,
b. die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,
c. die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,
d. die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,

e. die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,[345]

f. die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,

g. die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,

h. die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,

i. die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder

345 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 9 DSGVO.

j. die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich.

(3) Die in Absatz 1 genannten personenbezogenen Daten dürfen zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.

(4) Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.[346]

Nach Maßgabe des Art. 5 Abs. 2 DS-GVO muss der Verantwortliche im Rahmen seiner Rechenschaftspflicht die Einhaltung der Verarbeitungsgrundsätze des Abs.1 nachweisen können. Gelingt dieser Nachweis nicht, droht ebenfalls eine Geldbuße nach Art. 83 Abs. 5 lit. a DS-GVO.[347]

Der Grundsatz der Rechtmäßigkeit enthält kein Verbotsprinzip, wie vielfach unterstellt wird. Die Datenverarbeitung ist nicht grundsätzlich verboten, sondern unter bestimmten, in den datenschutzrechtlichen Erlaubnistatbeständen genannten Bedingungen erlaubt. Den Erlaubnistatbeständen liegen Abwägungen des Grundrechts auf Datenschutz mit

346 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art 9 DSGVO.

347 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, S. 213, Rn. 2.

anderen Grundrechten zugrunde. [348] Damit basiert das Datenschutzrecht weiterhin auf dem Verbotsprinzip, wonach jede Datenverarbeitung legalisiert werden muss. Die Zulässigkeit der Datenverarbeitung ergibt sich nach der DS-GVO aus den Art. 6 bis 11 sowie aus Art. 23 (automatisierte Einzelentscheidung) und Art. 44 ff. (Drittlandstransfer).[349]

3.2 Verarbeitung nach Treu und Glaube, (Art. 5 Abs.1 lit. a Alt. 2 DS-GVO)

Personenbezogene Daten sind gemäß Art. 5 Abs. 1 lit. a Var. 2 DS-GVO "**nach Treu und Glauben**" zu verarbeiten[350] Der Grundsatz Treu und Glauben findet sich in Nr. 108 der Konvention des Europarates, ist in Art. 8 Abs. 2 S. 1 der Europäischen-Grundrechtecharta verbürgt und wurde durch Art. 6 Abs. 1 der DSRL i.V.m. **Erwägungsgrund 38** DSRL ausgefüllt.[351]

Auch wenn das Gebot von Treu und Glauben unter der DS-GVO inhaltlich schwer zu fassen ist, verbietet es sich einfach auf den im deutschen nationalen Recht bestimmten Begriff von Treu und Glauben zurückzugreifen. Ein solches Vorgehen widerspricht dem unionsrechtlichen Grundsatz, dass das Unionsrecht eine eigenständige Rechtsordnung aufstellt, „nach der sich die Befugnisse, Rechte und Pflichten der Rechtssubjekte sowie die zur Feststellung und Ahndung etwaiger Rechtsverletzungen erforderlichen Verfahren bestimmen." Der Begriff von Treu und Glauben muss autonom für die DS-GVO als EU-Norm ausgelegt werden. Es kann nicht die Absicht des Gesetzgebers der EU gewesen sein, in Art. 5 Abs. 1 lit. a Var. 2 die vielseitigen Bedeutungsinhalte zu implementieren, die sich im Laufe der Zeit in der deutschen Rechtsordnung mit dem Begriff von Treu und Glauben entwickelt haben.[352]

348 *J. Philipp Albrecht,* Datenschutzrecht, S. 370, Rn. 35.
349 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 7620 von 87533, Rn. 21.
350 *Kühling/Klar/Sackmann,* Datenschutzrecht, 4. Aufl. 2018, S. 145, Abs. II, Rn. 335.
351 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 7620 von 87533, Rn. 25, Satz 2.
352 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 7620 von 87533, Rn. 26.

3.3 Transparenz (Art. 5 Abs. 1 lit. a Alt. 3 DS-GVO)

Nach Abs. 1 lit. a Alt.3 müssen personenbezogene Daten „in einer für die betroffene Person nachvollziehbare Weise“ verarbeitet werden. Der **Grundsatz der Transparenz** ist durch Art. 8 Abs. 2 S. 2 GRCh in der Weise primärrechtliche explizit abgesichert, als dieser Regelung jede Person das Recht gewährleistet, Auskunft über die sie betreffenden erhobenen Datum zu erhalten. Insoweit liegt Art. 8 Abs. 2 GRCh den einschlägigen Regelungen der DS-GVO zugrunde.[353]

Wer keine Kenntnisse über die Existenz von Datenverarbeitungsvorgängen hat, kann seine ihm zustehenden Rechte zum Schutz seiner Persönlichkeit, etwas die **Berichtigung** (Art. 16 DS-GVO), **Löschung** (Art. 17 DS-GVO, § 35 BDSG) oder **Einschränkungen der Verarbeitung** (Art. 18 DS-GVO) nicht wahrnehmen.[354]

Besondere Bedeutung kommt dem Transparenzerfordernis in Situationen zu, wo die große Zahl der Beteiligten und die Komplexität der dazu benötigten Technik den Betroffenen nicht ohne weiteres erkennen lassen, ob, von wem und zu welchem Zweck ihn betreffende personenbezogene Daten erfasst werden. Der Grundsatz transparenter Verarbeitung personenbezogener Daten wird von der DS-GVO somit als Gebot verstanden, dass die betroffene Person die Verarbeitung nachvollziehen können muss. Eine Pflicht zu kleinteiliger Information über jedes Detail der Verarbeitung im Voraus folgt aus dem Transparenzgrundsatz nicht.[355]

Die inhaltlichen Anforderungen ergeben sich vor allem aus den Informationspflichten der Art. 12, 13 und 14. Diese gehen über die Angaben zum Verantwortlichen, Zwecken der Verarbeitung Kategorie von Empfängern hinaus (so § 4 Abs. 3 BDSG a.F.),[356] indem grundsätzlich auch eine umfangreiche Information, insbesondere über die Rechte der Betroffenen Person, zu erfolgen hat. Im Rahmen der Informationspflichten ist es nach Ansicht der Art. 29-Datenschutzgruppe sogar notwendig, dass die Transparenzinformationen gegenüber betroffenen Personen regelmäßig aufzufrischen sind. Dies sei auch dann notwendig, wenn sich inhaltlich keine Änderungen ergeben

353 *J. Philipp Albrecht,* Datenschutzrecht, S. 373, Rn. 49.
354 *Kühling/Klar/Sackmann,* Datenschutzrecht, 4. Aufl. 2018, S. 146, Rn. 336.
355 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 7717 von 87533, Rn. 33.
356 *Körffer et al.,* Bundesdatenschutzgesetz, 10. Aufl. 2010, § 4 Abs. 3 BDSG (a,F.).

haben. Dem ist entgegenzuhalten, dass betroffene Personen, die keinen Überblick mehr über die **Transparenzinformationen** haben, sich diesen im Rahmen des Auskunftsersuchens gem. Art. 15 DS-GVO[357] verschaffen können. Sämtliche Betroffene ungefragt in regelmäßigen Abständen mit Informationen zu behelligen führt lediglich zu „transparency fatigue". Die Informationen würden dann bei tatsächlicher inhaltlicher Änderung gar nicht mehr zur Kenntnis genommen. Zudem erscheint es unbillig, Verantwortliche gem. Art. 83 DS-GVO für etwas haften zu lassen, dass in den Art. 13 und 14 nicht vorgeschrieben ist.[358]

Erweitert wurde auch das Auskunftsrecht der **betroffenen Person** (Art. 15). Weitere Konkretisierungen des **Grundsatzes der Transparenz** finden sich in der **Verpflichtung zur Benachrichtigung** des Betroffenen von Datenschutzverstößen (Art. 34) und der Veröffentlichung der Angaben zum betrieblichen oder behördlichen Datenschutzbeauftragten (Art. 37 Abs. 7).[359] [360]

Wesentliches Ziel von Zertifizierungen der Datenschutzkonformität ist die Transparenz. Nach **Erwägungsgrund 100** sollen Zertifizierungsverfahren sowie Datenschutzsiegel und- Prüfzeichen ermöglichen, den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen zu ermöglichen. Das Zertifizierungsverfahren ist seinerseits in Art. 42 geregelt. Diese Transparenzpflichten werden auf Grundlage der Öffnungsklausel in Art. 23 konkretisiert bzw. eingeschränkt in den §§ 23 bis 36 BDSG n.F. sowie bei der Videoüberwachung öffentlich zugänglicher Räume in § 4 Abs. 2 BDSG n.F.[361]

Erwägungsgrund 100

---

357 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 15 DSGVO.

358 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 7717 von 87533, Rn. 34.

359 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 7 Abs. 3, DSGVO.

360 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 7717 von 87533, Rn. 35.

361 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 7717 von 87533, Rn. 36.

Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsverfahren sowie Datenschutzsiegel und -Prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen.[362]

3.4 Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO)

Ein weiteres zentrales und seit jeher im deutschen Datenschutzrecht verankertes Regelungselement ist der Zweckbindungsgrundsatz. Er entspringt dem datenschutzrechtlichen Konzept der normativen Zweckbegrenzung. Gemäß Art. 5 Abs. 1 lit. b DS-GVO müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarten Weise weiterverarbeitet werden.[363]

Eine bestimmte Form ist für die Zweckfestlegung nicht vorgeschrieben. Es ist aber zu berücksichtigen, dass der Verantwortliche nach Art. 5 Abs. 2 die Einhaltung des Zweckbindungsgrundsatzes nachweisen können muss. Eine rein gedankliche Zweckfestlegung wird hierzu nicht ausreichen. Vielmehr muss die Festlegung in einer Weise dokumentiert werden, die es Dritten erlaubt, sie nachzuvollziehen. Geeignet ist hierfür jedenfalls die Dokumentation der Verarbeitungswecke in Schriftform. Sofern andere Formen die notwendige Nachweisfunktion erfüllen, sind auch diese Formen praktikabel.[364]

Mögliches Einfallstor für eine solche Aufweichung ist zunächst einmal die Einschränkung in Art. 5 Abs. 1 lit. b, wonach eine Weiterverarbeitung von Daten für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche, historische oder statistische Zwecke nicht als unvereinbar mit den ursprünglichen Zwecken gilt. Jedoch ist diese Öffnung von vornherein eng zu verstehen, nicht nur weil sie der Sache nach eine – vom Gesetzgeber gewünschte – Ausnahme vom Zweckbindungsgrundsatz darstellt,

362 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 100.

363 *Kühling/Klar/Sackmann,* Datenschutzrecht, 4. Aufl. 2018, Seite 146, Rn. 338.

364 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, 7723 von 87533, Rn.39.

sondern vor allem auch mit Blick auf die detaillierten Ausführungen in den **Erwägungsgründen 125** ff., die deutlich machen, dass solcherlei Zwecksetzungen hohen Anforderungen genügen müssen. Keinesfalls reicht es aus, dass lediglich die Datenverarbeitung selbst eine irgendwie geartete wissenschaftliche, historische oder statistische Methode darstellt. Daher ist es auch von vornherein ausgeschlossen, dass etwa Profiling- und Scoring Verfahren oder Big Data-Analysen als „Statistik" vom Zweckbindungsgrundsatz ausgenommen sind.[365]

Ein zweites mögliches Einfallstor für eine Aufweichung des Zweckbindungsgrundsatzes ist daneben die Regelung in Art. 6 Abs. 3a, wonach anhand von fünf Kriterien zu bestimmen ist, ob die Datenverarbeitung zu einem anderen Zweck als dem ursprünglich verfolgten gleichwohl noch mit dem ursprünglichen Erhebungszweck vereinbar ist. Berücksichtigt werden sollen hierfür: jede Verbindung („any link") zwischen ursprünglichem Erhebungszweck und weiteren Verarbeitungszwecken, der Kontext der Datenerhebung, die Art der Daten, mögliche Konsequenzen der beabsichtigten Datenverarbeitung für den Betroffenen sowie das Vorhandensein angemessener Schutzmaßnahmen wie etwa Verschlüsselung oder Pseudonymisierung. Aus Sicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder macht die Regelung Zweckänderungen in einem derart weiten Umfang zulässig, dass dies einer Preisgabe des in der Europäischen Grundrechtecharta enthaltenen Prinzips der Zweckbindung gleichkommt.[366]

Ob eine solche Preisgabe tatsächlich zu befürchten ist, wird vor allem auch davon abhängen, wie streng oder großzügig die Anforderungen an die ursprüngliche Zwecksetzung nach Art. 5 Abs. 1 lit. b („festgelegt" und „eindeutig") ausgelegt werden. Je höher die Anforderungen an die Festlegung und Eindeutigkeit der ursprünglichen Zwecksetzung sind, desto geringer ist dann auch das Risiko einer Aufweichung über Art. 6 Abs. 3a.

365 *DuD* Datenschutz Datensich 2016, 155 (Seite. 157).
366 *DuD* Datenschutz Datensich 2016, 155 (Seite.155 - 156).

Erwägungsgrund 125

Die federführende Behörde sollte berechtigt sein, verbindliche Beschlüsse über Maßnahmen zu erlassen, mit denen die ihr gemäß dieser Verordnung übertragenen Befugnisse ausgeübt werden. In ihrer Eigenschaft als federführende Behörde sollte diese Aufsichtsbehörde für die enge Einbindung und Koordinierung der betroffenen Aufsichtsbehörden im Entscheidungsprozess sorgen. Wird beschlossen, die Beschwerde der betroffenen Person vollständig oder teilweise abzuweisen, so sollte dieser Beschluss von der Aufsichtsbehörde angenommen werden, bei der die Beschwerde eingelegt wurde.[367]

3.5 Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO)

Gemäß Art. 5 Abs. 1 lit. c müssen personenbezogenen Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Zusammenfassend bezeichnet die DS-GVO diesen **Grundsatz als „Datenminimierung**". Nach der DS-GVO unzulässig ist damit die Verarbeitung personenbezogener Daten, die für den verfolgten Zweck inadäquat, unerheblich oder entbehrlich sind.

Die drei Merkmale „**angemessen**", „**erheblich**" und „**auf das notwendige Maß beschränk**t" sind kaum trennscharf zu definieren; zusammengenommen ergeben sie eine Anforderung, die auch formuliert werden könnte als „zur Erreichung des festgelegten Verarbeitungszwecks erforderlich". Dennoch klingen in den drei Merkmalen unterschiedliche Aspekte dieser Anforderung an. So sind Daten dem Zweck angemessen, wenn sie überhaupt einen Bezug zum Verarbeitungszweck haben, und sie sind erheblich, wenn ihre Verarbeitung geeignet ist, den festgelegten Zweck zu fördern.[368]

Unternehmen dürfen somit nur so viele Daten verarbeiten, wie es der Zweck der jeweiligen Datenverarbeitung erfordert. Auch die Intensität der Datenverarbeitung muss auf das für die Zweckerreichung notwendige Maß beschränkt sein.[369]

---

367 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 125.

368 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, S. 208, Rn. 57.

369 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 23, Rn. 71.

Bei der Prüfung des **Grundsatzes der Datenminimierung** ist insbesondere zu bedenken, ob der Verarbeitungszweck auch dann erreicht werden kann, wenn die Daten anonymisiert sind; denn dann sind die Daten nicht mehr personenbezogen und somit nicht dem Grundsatz der Datenminimierung unterworfen.[370]

3.6 Rechtsbehelfe / Haftung / Sanktionen (Art. 77 bis 84 DS-GVO)

Rechtsbehelfe, Haftung und Sanktionen sind im Kapitel VIII der DS-GVO geregelt (Art. 77 bis 84 DS-GVO). Sie werden durch die Erwägungsgründe 141 – 152 ergänzt. Systematisch wählt das neue EU-Recht einen **Dreiklang** aus Rechtbehelfen.

Rechtswege:

- Beschwerde bei Aufsichtsbehörde
- Gerichtsverfahren gegen Aufsichtsbehörde
- Gerichtsverfahren gegen Verantwortlichen / Auftragsverarbeiter

Vertretung:

- Vertretung des Betroffenen durch einen Verband
- Verbandsklagerecht (nach nationalem Recht)

Sanktionen:

- Schadenersatz
- Bußgeld
- Strafe (nach nationalem Recht)

Abs. 1 des Artikel 83 der Datenschutz-Grundverordnung führt aus, dass jede Aufsichtsbehörde sicherstellen muss, dass die Verhängung von **Geldbußen** in jedem Einzelfall **wirksam**, **verhältnismäßig** und **abschreckend** ist.[371]

Bereits vor Einführung der Datenschutz-Grundverordnung wurde über exorbitante Bußgelder berichtet. Bußgelder für Datenschutzverstöße sind nicht neu, so sah schon das

370 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, Seite 208, Rn. 58.

371 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 83 Abs. 1 DSGVO.

noch geltende Bundesdatenschutzgesetz (BDSG-alte Fassung) durchaus Bußgelder für Datenschutzverstöße vor. Die deutschen Datenschutzbehörden haben hiervon in der Vergangenheit jedoch keinen extensiven Gebrauch gemacht. Die Resonanz in der Praxis liegt daher bisher zwischen „Handeln mit Augenmaß“ und „Bußgelder drohen gar nicht“.[372]

Aus diesem Grund würde zur Modernisierung unbedingt auch eine bessere Handhabung des Gesetzes einerseits i.V.m. einer griffigen Haftungsregelung anderseits gehören. Sowohl strafrechtlich als auch haftungsrechtlich erscheint es unangemessen, bei den zahlreichen und sehr schwer zu handhabenden Regel-/Ausnahmen- und Rücknahmeregelungen genau zu ermitteln, was zulässig ist und was unzulässig ist. Die Schwierigkeit der Einschätzung und die zum Teil sehr heterogenen Meinungen dazu dürfen im konkreten Fall bei der Ermittlung von Vorsatz und grober Fahrlässigkeit eine erhebliche Rolle spielen.[373]

Die Datenschutz-Grundverordnung erhöht gegenüber dem BDSG (alt) den Bußgeldrahmen um das **60-fache**. Das „große Bußgeld“ beträgt nach Art. 83 Abs. 5 DS-GVO bis zu 20 Mio. Euro oder im Fall eines Unternehmens bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs – je nachdem, welcher Betrag höher ist. Das „große Bußgeld“ kommt bei Verstößen gegen die in Art. 83 Abs. 5 DS-GVO genannten Pflichten zum Tragen. Das „kleine Bußgeld“ beträgt immer noch bis zu 10 Mio. Euro bzw. 2 % des Umsatzes und greift bei Verstößen gegen die in Art. 83 Abs. 3 DS-GVO genannten Pflichten. Nach Art. 83 Abs. 6 DS-GVO droht ebenfalls ein „großes Bußgeld“ bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Art. 58 Abs. 2 DS-GVO.[374]

372 [Der Titel "DuD, Datenschutz und Datensicherheit" kann nicht dargestellt werden. Die Vorlage "Fußnote - Zeitschriftenaufsatz - (Standardvorlage)" beinhaltet nur Felder, welche bei diesem Titel leer sind.]

373 *Forgó/Helfrich/Schneider* (Hrsg.), Betrieblicher Datenschutz, S. 37, Rn. 128 Abs. 1.

374 [Der Titel "DuD, Datenschutz und Datensicherheit" kann nicht dargestellt werden. Die Vorlage "Fußnote - Zeitschriftenaufsatz - (Standardvorlage)" beinhaltet nur Felder, welche bei diesem Titel leer sind.]

3.7 Richtigkeit (Art. 5 Abs. 1 lit. d DS-GVO)

Ein unrichtiger Speicherinhalt macht sich bei der Auslesung, Abfrage, Verwendung und Weitergabe bemerkbar und soll daher vermieden werden. Unter dem Schlagwort „Richtigkeit“ sind daher drei Grundpflichten normiert:

- Das Verbot der unrichtigen Erhebung oder Speicherung von Daten (Hs. 1 Var. 1),
- das Gebot der Aktualisierung unrichtig gewordener Daten (Hs. 1 Var. 2) und
- das Gebot der Löschung oder Berichtigung unrichtig gespeicherter Daten (Hs. 2).[375]

Nach Art. 5 Abs. 1 lit. d müssen personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neusten Stand sein. „**Sachlich richtig**“ ist ein **objektives Kriterium** und bedeutet, dass die über die betroffene Person gespeicherten Informationen mit der Realität übereinstimmen (vgl. Art. 16 Rn. 8 ff.[376]).[377]

Das Gebot der Aktualisierung unrichtig gewordener Daten beinhaltet nach Art. 5 Abs. 1 lit. d Hs. 1 Var. 2 Aktualisierungspflichten vor allem in den Fällen, in denen Daten aus berechtigten Gründen zulässig längere Zeit aufbewahrt werden. In Betracht kommen hier neben Behörden namentlich Unternehmen, die – wie Auskunfteien, Detekteien oder Unternehmen bei Dauerschuldverhältnissen – personenbezogene Daten längerfristig aufbewahren. Im Rahmen des Profiling konkretisiert **Erwägungsgrund 71** das Aktualisierungsgebot. Danach hat der Verantwortliche die Aufgabe technische und organisatorische Maßnahmen zu treffen, mit denen in geeigneter Weise sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird.[378]

---

375 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, Seite.327, Rn. 34.

376 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 16 Rn.8 ff.

377 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, Seite 209, Rn. 60.

378 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 7876 von 87533, Rn. 55.

Der **Grundsatz der Richtigkeit** wird jedoch relativiert durch den Zusatz „erforderlichenfalls“ in Art. 5 Abs. 1 lit. d Hs. 1 Var. 2.[379] Damit müssen die personenbezogenen Daten **nicht in jedem Fall** auf dem **neuesten Stand** sein. Werden beispielsweise Gesundheitsdaten einer betroffenen Person bei einer bestimmten Untersuchung gewonnen, kann sich deren Richtigkeit logischerweise nur auf den Zeitpunkt der Untersuchung beziehen. Eine Berichtigung ist ebenfalls nicht erforderlich, wenn das betreffende Datum zu Zwecken der Beweissicherung auf Grundlage der Interessenabwägung gemäß Art. 6 Abs. 1 lit. f [380] notwendig ist.[381]

Das Kriterium der Richtigkeit muss sich dabei an den Verarbeitungszwecken orientieren. Die Richtigkeit muss im Hinblick auf die Zwecke der Verarbeitung gegeben sein. Eine Berichtigung ist nicht erforderlich, wenn das Datum mit Blick auf die Verarbeitungszwecke in seiner konkreten Ausgestaltung im Detail nicht relevant ist. Falls richtige Daten unter dem Grundsatz der Datenminimierung nicht notwendig sind, besteht insoweit ebenfalls keine Verpflichtung zur Gewährleistung der Richtigkeit.[382]

Der Grundsatz der Richtigkeit korrespondiert mit den Rechten der betroffenen Person auf **Berichtigung** (Art. 16) [383], **Löschung** (Art. 17) und **Einschränkung der Verarbeitung** (Art. 18). Diese Eigenschaften sind in der Form als Betroffenenrechte ausgestaltet. [384]

Erwägungsgrund 71

---

379 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 5 Abs. 1 lit. d Hs. 1 Var. 2 DSGVO.

380 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 6 Abs. 1 lit. f DSGVO.

381 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 7876 von 87533, Rn. 56.

382 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 7876 von 87533, Rn. 57.

383 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 16 DSGVO.

384 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 7884 von 87533, Rn. 58.

Die betroffene Person sollte das Recht haben, keiner Entscheidung - was eine Maßnahme einschließen kann - zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wie die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen. Zu einer derartigen Verarbeitung zählt auch das "Profiling", das in jeglicher Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person besteht, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Eine auf einer derartigen Verarbeitung, einschließlich des Profiling, beruhende Entscheidungsfindung sollte allerdings erlaubt sein, wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der für die Verarbeitung Verantwortliche unterliegt, ausdrücklich zulässig ist, auch um im Einklang mit den Vorschriften, Standards und Empfehlungen der Institutionen der Union oder der nationalen Aufsichtsgremien Betrug und Steuerhinterziehung zu überwachen und zu verhindern und die Sicherheit und Zuverlässigkeit eines von dem Verantwortlichen bereitgestellten Dienstes zu gewährleisten, oder wenn dies für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und einem Verantwortlichen erforderlich ist oder wenn die betroffene Person ihre ausdrückliche Einwilligung hierzu erteilt hat. In jedem Fall sollte eine solche Verarbeitung mit angemessenen Garantien verbunden sein, einschließlich der spezifischen Unterrichtung der betroffenen Person und des Anspruchs auf direktes Eingreifen einer Person, auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung sowie des Rechts auf Anfechtung der Entscheidung. Diese Maßnahme sollte kein Kind betreffen.

Um unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten, sollte der für die Verarbeitung Verantwortliche geeignete mathematische oder statistische Verfahren für das Profiling verwenden, technische und organisatorische Maßnahmen treffen, mit denen

in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird, und personenbezogene Daten in einer Weise sichern, dass den potenziellen Bedrohungen für die Interessen und Rechte der betroffenen Person Rechnung getragen wird und unter anderem verhindern, dass es gegenüber natürlichen Personen aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetischer Anlagen oder Gesundheitszustand sowie sexueller Orientierung zu diskriminierenden Wirkungen oder zu einer Verarbeitung kommt, die eine solche Wirkung hat. Automatisierte Entscheidungsfindung und Profiling auf der Grundlage besonderer Kategorien von personenbezogenen Daten sollten nur unter bestimmten Bedingungen erlaubt sein.[385]

385 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 71.

3.8 Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO)

Nach Abs. 1 lit. e müssen personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Durch den Grundsatz der Speicherbegrenzung wird der Grundsatz der Zweckbindung und das **Verhältnismäßigkeitsprinzip** in zeitlicher Hinsicht konkretisiert. Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen.[386]

Erwägungsgrund 39 ermöglicht hierzu tiefergehende Einblicke in die Begrenzung der Speicher:

Jede Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen. Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden. Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können. Insbesondere sollten die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen. Die personenbezogenen Daten sollten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie

386 *Gola u. a.* (Hrsg.), Datenschutz-Grundverordnung, Seite 193, Rn. 25.

auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen. Es sollten alle vertretbaren Schritte unternommen werden, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden. Personenbezogene Daten sollten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.[387]

3.9 Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DS-GVO)

Nach Art. 5 Abs.1 lit. f müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine **angemessene Sicherheit** der personenbezogenen Daten gewährleistet.

Hierfür sollen insbesondere geeignete technische und organisatorische Maßnahmen eingesetzt werden, um vorbestimmten, in den einzelnen genannten Risiken zu schützen.[388]

Zum einen sollen Integrität und Vertraulichkeit den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung gewährleisten. Eine unrechtmäßige Verarbeitung liegt vor, wenn hierfür keine Rechtsgrundlage vorliegt. Eine unbefugte Verarbeitung ist gegeben, wenn ein Dritter im Sinne von Art. 4 Nr. 10 ohne Befugnis eine Datenverarbeitung vornimmt. Deshalb ist durch **t**echnisch **o**rganisatorische **M**aßnahmen (**TOM**) der unbefugte Zugang zu personenbezogenen Daten zu verhindern.[389]

---

387 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 39.

388 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, Seite 210, Rn.72+73.

389 *Bäcker,* Datenschutz-Grundverordnung, Herbst, S. 211, Rn. 74.

Daneben soll ein unbeabsichtigter Verlust, eine unbeabsichtigte Zerstörung oder eine unbeabsichtigte Schädigung verhindert werden. Ein unbeabsichtigter Verlust, eine unbeabsichtigte Zerstörung oder unbeabsichtigte Schädigung von Daten liegt vor, wenn in der Sphäre des Verantwortlichen durch mit der Datenverarbeitung betrauten Personen Daten verlustig gehen, zerstört oder beschädigt werden. Das ist insbesondere dann der Fall, wenn Daten abhandenkommen oder derart geändert werden, dass sie nicht mehr oder nur noch eingeschränkt für den vorgesehenen Zweck verarbeitet werden können. Welche Maßnahmen zum Schutz der Daten ergriffen werden müssen, hängt insbesondere von dem Risiko eines unberechtigten Zugriffs, der Art der Verarbeitung[390] sowie der Bedeutung der Daten für die Rechte und Interessen der betroffenen Personen ab. So werden beispielsweise persönliche Finanz- oder Gesundheitsdaten eines höheren Schutzes bedürfen als der Name oder das Alter einer Person. Nach Erwägungsgrund 39 gehört zu den Schutzmaßnahmen zumindest, dass personenbezogene Daten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.[391]

390 Große Kammer, 13.5.2014 – C-131/12 Neue Juristische Wochenschrift 2014, 2225.
391 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, 7930 von 87533, Rn. 66 - 69.

3.10 Rechenschaftspflicht (Art. 5 Abs. 1 lit. b DS-GVO)

Die **Rechenschaftspflicht** (Art. 5 Abs. 2) ist das schillerndste Gebot der EU-Datenschutz-Grundverordnung[392]. Schon in der EG-Datenschutz-Richtlinie[393] (Art. 6 Abs. 2) findet sich der Grundsatz, dass der Verantwortliche für die Einhaltung der Datenschutzgrundsätze verantwortlich ist. Zunächst einmal stellt die EU-Datenschutz-Grundverordnung mit dieser redundanten Formulierung klar, dass die Pflichten aus den Datenschutzgrundsätzen den Verantwortlichen (Art. 4 Ziffer 7) treffen.[394]

Die **Rechenschaftspflicht** des Art. 5 Abs. 2 ist eines der gewichtigsten und umfänglichsten Gebote der DS-GVO. Die Rechenschaftspflicht des Verantwortlichen nach Art. 5 Abs. 2 hat zwei Bestandteile: Die Einhaltung der Grundsätze des Art. 5 Abs. 1 wird ihm als Pflicht auferlegt, und er muss nachweisen können, dass er diese Pflicht befolgt. Art. 5 Abs. 2 enthält damit die beiden wesentlichen Aspekte des Konzepts der „Accountability". Über den Grundsatz der Rechenschaftspflicht bekommt Art. 5 eine hohe eigenständige Bedeutung mit erheblicher Praxisrelevanz.[395]

Der Grundsatz der Rechenschaftspflicht war als Verpflichtung, die Einhaltung der Grundsätze des Art. 6 Abs. 1 DSRL sicherzustellen, bereits in Art. 6 Abs. 2 DSRL enthalten. Die Verpflichtung des Verantwortlichen, die Einhaltung der Grundsätze nun auch nachweisen zu müssen, ist dagegen ein Novum im Rahmen der DS-GVO. Mit dem Grundsatz der Rechenschaftspflicht nimmt der Gesetzgeber die Verantwortlichen stärker in die Pflicht. Statt einer bürokratischen Vorabkontrolle möchte er stärker auf die Eigenverantwortung der Verantwortlichen setzen und diese als sanktionsbewehrten Grundsatz zum Fundament des neuen Datenschutzrechts machen.[396]

---

392 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).

393 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates.

394 *Assion/Brüggemann,* DSGVO, BDSG, Seite 104, Rn. 33.

395 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 7990 von 87533, Rn. 72.

396 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, 7990 von 87533, Rn. 73.

Während die EG-Datenschutzrichtlinie eine Rechenschaftspflicht nicht ausdrücklich vorsah, führt die DS-GVO dieses Grundprinzip in Art. 5 Abs. 2 DS-GVO ein. Danach obliegt die Verantwortlichkeit für die Einhaltung der Vorgaben der DS-GVO in Bezug auf die Verarbeitungstätigkeiten sowie die Pflicht zum Nachweis dieser Einhaltung dem Verantwortlichen. Das Prinzip der Rechenschaftspflicht besteht aus zwei Elementen:

1. Die Verpflichtung des Verantwortlichen, die Einhaltung der DS-GVO sicherzustellen; und
2. Die Befähigung des Verantwortlichen, diese Einhaltung gegenüber den Aufsichtsbehörden nachzuweisen.[397]

Die **Dokumentation und Rechenschaft** betreffen auch die Auseinandersetzung der Datenschutzaufsichtsbehörde mit ihrer Schwerpunktsetzung, ihrer Ausstattung und der Verteilung der vorhandenen Ressourcen. Anhand dieser Dokumentation können Kapazitätsgrenzen der Datenschutzaufsichtsbehörde aufgezeigt werden, um diese zukünftig im Haushalt besser auszustatten und sicherzustellen, dass den Vorgaben des Art. 52 Abs. 4 (Art. 52 Rn. 41 ff.) entsprochen wird.[398]

3.10.1 Verantwortlichkeit (HS. 1)

Wie schon Art. 6 Abs. 2 DSRL regelt Art. 5 Abs. 2 HS. 1 DS-GVO, dass der Verantwortliche für die Einhaltung der Grundsätze des Abs.1 zu sorgen hat. Verstärkt wird diese Regelung durch die Bußgeldbewährung in Art. 83 Abs. 5 lit. a.[399]

3.10.2 Nachweispflicht (HS. 2)

Der Verantwortliche muss die Einhaltung der Grundsätze des Abs.1 auch nachweisen können. Diese Nachweispflicht hat insbes. Bedeutung im Hinblick auf Überprüfung durch die Aufsichtsbehörden, die nach Art. 58 Abs. 1 lit. a auch die Befugnisse haben, den Verantwortlichen zur Bereitstellung von Informationen anzuweisen. Kann der Verantwortliche die Einhaltung der Grundsätze des Art. 5 Abs. 1 nicht nachweisen, dann

397 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, Rechenschaftspflicht, S. 39, 3.1.
398 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Rechenschaft und Transparenz, Position. 61203 von 87533, Rn. 11.
399 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, Seite.211 Rn. 78.

geht dies jedenfalls als Verletzung der Nachweispflicht aus Art. 5 Abs. 2 Hs. 2 zu seinen Lasten; nach Art. 82 Abs. 3 kann er sich dann auch nicht von einer Haftung befreien.[400]

3.10.3 Unabhängige Kontrolle

Obwohl Art. 5 DS-GVO die unabhängige Kontrolle nicht nennt, gehört sie zu den tragenden Grundsätzen des europäischen Datenschutzrechts. Anders als bei den Grundsätzen aus Art. 5 DS-GVO handelt es sich jedoch um keine Vorgabe, die die Beteiligten bei der Verarbeitung personenbezogener Daten einhalten müssen, sondern um ein überindividuelles allgemeines Strukturprinzip des Datenschutzrechts.[401]

Schon das BVerfG hat im Volkszählungsurteil hervorgehoben, dass Betroffene die Abläufe und das Vorhandensein von Datenverarbeitungsvorgängen selbst kaum überblicken können.[402] Die Kontrolle der Verarbeitung durch unabhängige Stellen ist deshalb ein „wesentlicher Bestandteil“ für einen effektiven Datenschutz den das Primärrecht verbürgt, Art. 8 Abs. 3 GRCh i.V.m Art. 16 Abs. 2 S. 2 AEUV. Die „**volle Unabhängigkeit**“ der Aufsichtsbehörden hat auch der EuGH bereits mehrfach gestärkt. [403]

In ständiger Rechtsprechung fordert er, dass die Aufsicht „völlig frei von Weisungen und Druck handeln“ können muss, damit sie ihre Aufgaben „objektiv und unparteiisch“[404] wahrnimmt. Hierzu gehört nicht nur die Eigenständigkeit gegenüber den kontrollierten Stellen,[405] sondern auch die gegenüber staatlichen Stellen.[406]

---

400 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, Seite 211. Rn. 79.
401 *Conseil de l'Europe*, SEV 181 - Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr.Klicken oder tippen Sie hier, um Text einzugeben.
402 *Bundesverfassungsgericht/Senat* (E 65, 1, 46 - Volkszählung).
403 *Rechtssache C-362/14*.
404 [Der Titel "" kann nicht dargestellt werden. Die Vorlage "Fußnote - Gesetz / Verordnung in Zeitschrift - (Standardvorlage)" beinhaltet nur Felder, welche bei diesem Titel leer sind.]
405 EuGH – Rs. C-518/07.
406 [Der Titel "" kann nicht dargestellt werden. Die Vorlage "Fußnote - Gesetz / Verordnung in Zeitschrift - (Standardvorlage)" beinhaltet nur Felder, welche bei diesem Titel leer sind.]

3.11 Rechtswege (Art. 78 Abs. 1 DS-GVO)

Gegen Entscheidungen der Aufsichtsbehörden steht gemäß Art. 78 Abs. 1 der Rechtsweg offen. Für Klagen gegen Entscheidungen der deutschen Aufsichtsbehörden ist das Verwaltungsgericht zuständig, in dessen Bezirk die Aufsichtsbehörde ihren Sitz hat (vgl. Art. 78 Abs. 1 i.V.m. § 21 BDSG). Kommt es innerhalb des **Kohärenzverfahrens** zu einem verbindlichen Beschluss des Datenschutzausschusses (Art. 65)[407], kann der Rechtsweg nach Art. 263 AEUV eröffnet sein. Voraussetzung ist, dass Beschlüsse des Ausschusses einen Verantwortlichen, einen Auftragsverarbeiter oder den Beschwerdeführer unmittelbar und individuell betreffen. Dies wird bei einem Unternehmen, dessen verbindliche interne Datenschutzvorschriften vom Datenschutzausschuss für nicht genehmigungsfähig erklärt wurden, regelmäßig der Fall sein. Eine solche Klage müsste **binnen zwei Monaten** nach Veröffentlichung der betreffenden Beschlüsse erhoben werden.[408]

Gemäß Art. 78 DS-GVO hat jede betroffene Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen die Aufsichtsbehörden. Genau wie Verantwortliche / Auftragsverarbeiter können betroffene Personen gegen sie betreffende rechtsverbindliche Beschlüsse der Aufsichtsbehörden nach Art. 78 Abs. 1 DS-GVO vorgehen. Zudem hat jede betroffene Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn die zuständige Aufsichtsbehörde sich nicht mit ihrer Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der nach Art. 77 DS-GVO erhobenen Beschwerde in Kenntnis gesetzt hat.[409]

In Bezug auf Verantwortliche / Auftragsverarbeiter hat jede betroffene Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund der DS-GVO zustehenden Rechte infolge einer nicht im Einklang mit der Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden, Art. 79 Abs. 1 DS-GVO. Dies gilt unbeschadet von verfügbaren verwaltungsrechtlichen

---

407 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 65 DSGVO.

408 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, 8870 von 14106.

409 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, 8833 von 14106.

oder außergerichtlichen Rechtsbehelfen im Recht der EU-Mitgliedstaaten. Derartige Klagen sind vor den Gerichten desjenigen EU-Mitgliedstaats zu erheben, in dem der Verantwortliche/Auftragsverarbeiter eine Niederlassung oder, wahlweise, wo die betroffene Person ihren Aufenthaltsort hat, siehe Art. 79 Abs. 2 DS-GVO.[410]

410 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, 8871 von 14106.

3.12 Der Datenschutzbeauftragte (Art. 37 – 39 DS-GVO)

Kapitel IV der DS-GVO regelt die Pflichten des Verantwortlichen und des Auftragsverarbeiters. In den Art. 37 - 39 DS-GVO ist der Datenschutzbeauftragte verortet. Sie regeln die Benennung (Art. 37 DS-GVO), die Stellung (Art. 38 DS-GVO) und die Aufgaben des Datenschutzbeauftragten (Art. 39 DS-GVO). Der Datenschutzbeauftragte ist ein Instrument der Selbstkontrolle, wie es auch andere Rechtsgebiete kennen, insbesondere das Umweltrecht.[411]

Die DS-GVO sieht in Art. 37 drei Konstellationen der Benennung von Datenschutzbeauftragten vor:

- Die unionsweite verpflichtende Benennung eines Datenschutzbeauftragten in den Fällen des Art. 37 Abs. 1 lit. a bis lit. c DS-GVO[412]
- Die nach nationalem Recht verpflichtende Benennung eines Datenschutzbeauftragten unter Nutzung der Öffnungsklausel in Art. 37 Abs. 4 Satz 1 HS. DS-GVO;
- Eine freiwillige Benennung eines Datenschutzbeauftragten Art. 37 Abs. 4 Satz 1 HS. 1 DS-GVO.

Darüber hinaus ist durch Art. 37 Abs. 2 DS-GVO gestattet, dass eine Unternehmensgruppe einen gemeinsamen Datenschutzbeauftragten ernennt, sofern von jeder Niederlassung aus dem Datenschutzbeauftragten leicht erreicht werden kann. [413]

Die Datenschutz-Grundverordnung sowie das BDSG-neue Fassung (das ab Mai 2018 geltende Bundesdatenschutzgesetz) sehen den Datenschutzbeauftragten nicht ausdrücklich als Adressat von Schadensersatz oder von Bußgeldern vor. Ausdrücklich werden in Art. 83 i.V.m. Art. 5, 6 DS-GVO der Verantwortliche und der Auftragsverarbeiter als **möglicher** Bußgeldadressaten genannt. Da die genannten

411 *Rüpke/K. Lewinski/Eckhardt,* Datenschutzrecht, 2018, 5 Abschnitt. Datenschutzkontrolle, §21 Interne Selbst–Kontrolle: Datenschutzbeauftragter, Rn. 1+2.

412 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 37 Abs. 1 lit. a bis lit. c DSGVO.

413 *Rüpke/K. Lewinski/Eckhardt,* Datenschutzrecht, 2018, Benennung eines Datenschutzbeauftragten, S. 293, Rn. 10.

Normen den Datenschutzbeauftragten nicht ausdrücklich nennen, stellt sich die Frage, ob an den Verantwortlichen und den Auftragsverarbeiter verhängte Bußgelder nach allgemeinem zivilrechtlichen Regelungen an den Datenschutzbeauftragten durchgereicht werden können.[414]

Eine Haftung des Datenschutzbeauftragten auf Grundlage von Art. 82 scheidet aus, da sich dieser nur an Verantwortliche und Auftragsverarbeiter richtet. Mangels abschließenden Charakters der Regelung kommen daneben aber vertragliche Haftungsansprüche bzw. Ansprüche aufgrund nationaler deliktischer Normen in Frage. Da mit dem internen Datenschutzbeauftragten ein Arbeitsverhältnis und mit dem externen Datenschutzbeauftragten ein Geschäftsbesorgungsvertrag (§ 675 BGB)[415] besteht, sind mögliche Rechtsgrundlagen für die Haftung gegenüber einem Verantwortlichen bzw. Auftragsverarbeiter regelmäßig § 280 Abs. 1 BGB, wobei ggf. eine Minderung der Haftung infolge Mitverschuldens (§ 254 BGB) des Verantwortlichen bzw. Auftragsverarbeiters zu bedenken sind. Rechtsgrundlage einer möglichen Haftung des Datenschutzbeauftragten im Verhältnis zur betroffenen Person ist § 823 Abs. 1 BGB bzw. § 823 Abs. 2 BGB i.V.m. Art. 39[416]. Auf Basis ihres Schutzzwecks (Art. 1 Abs. 1) sind die Normen der DS-GVO regelmäßig als deliktsrechtliche Schutzgesetze einzuordnen.[417]

Voraussetzung einer zivilrechtlichen Haftung des Datenschutzbeauftragten ist das Vorliegen einer **schuldhaften Pflichtverletzung durch** entweder ein **aktives Handeln** oder **ein Unterlassen**, wodurch ein kausaler Schaden entstanden sein muss. Dreh- und Angelpunkt einer schuldhaften Pflichtverletzung sind die Leistungspflichten des Datenschutzbeauftragten, da diese quasi den Haftungsrahmen bilden. Anders gesagt wird ohne eine Leistungspflicht keine Pflichtverletzung vorliegen und ohne eine Pflichtverletzung keine Haftung.[418]

---

414 [Der Titel "DuD, 3/2018" kann nicht dargestellt werden. Die Vorlage "Fußnote - Zeitschriftenaufsatz - (Standardvorlage)" beinhaltet nur Felder, welche bei diesem Titel leer sind.]

415 Bürgerliches Gesetzbuch, § 675 BGB.

416 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 39 DSGVO.

417 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Art. 39, Rn. 25, Haftung des Datenschutzbeauftragten.

418 *Steffen/DuD, 3/2018, S.145 Nr. 2. Zivilrechtliche Haftung von Datenschutzbeauftragten für Bußgelder* Datenschutz und Datensicherheit 2018, 145.

3.13 Umgang mit Betroffenen

Ein Bereich, in dem die DS-GVO größere Änderungen an der bisherigen Rechtslage vornimmt, ist der Bereich der Betroffenenrechte, also den Rechten, die Personen deren personenbezogenen Daten Gegenstand einer Datenverarbeitung sind, gegenüber dem für diese Datenverarbeitung Verantwortlichen zustehen.[419]

So wurden durch die DS-GVO zwei neue, in der Datenschutzrichtlinie 95/46/EG so bisher nicht vorgesehene Betroffenenrechte eingeführt: das Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO und das Recht auf Vergessenwerden nach Art. 17 DS-GVO. [420]

Außerdem wurden einige bestehende Betroffenenrechte, wie z.B. das Recht auf Auskunft und die Informationspflichten des Verantwortlichen, durch die DS-GVO erheblich erweitert und präzisiert.[421]

Hierzu werden die Artikel 12 bis Artikel 23 betrachtet und näher analysiert. Nachfolgende Kurzinformationen zeigen die ersten Betrachtungen.

1. Transparente Information und Kommunikation gegenüber betroffenen Personen (Art. 12 DS-GVO)
2. Informationspflichten bei Datenerhebung (Art. 13 und Art. 14 DS-GVO)
3. Auskunftsrechte betroffener Personen (Art. 15 DS-GVO)
4. Das Recht auf Berichtigung (Art. 16 DS-GVO)
5. Das Recht auf Löschung (Art. 17 DS-GVO)
6. Das Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO)
7. Das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO)
8. Widerspruchsrechte (Art. 21 DS-GVO)
9. Profiling und andere automatisierte Einzelentscheidungen (Art. 22 DS-GVO)
10. Die Möglichkeit der Beschränkung der Betroffenenrechte durch Rechtsvorschriften der Union oder der Mitgliedstaaten (Art. 23 DS-GVO)

419 De Gruyter Praxishandbuch, Seite. 141, Rn. 1.
420 De Gruyter Praxishandbuch, Seite. 141, Rn. 2.
421 *Moos/Schefzig/Arning* in, De Gruyter Praxishandbuch (Seite. 141, Rn. 3).

11. Art. 12 eröffnet Kapitel 3 der DS-GVO mit dem Titel „**Rechte der betroffenen Person**“ Als einzige Vorschrift des Abschnitt 1 „Transparenz und Modalitäten enthält Art. 12 allgemeine Anforderungen an die **Transparenz und Modalitäten** der Informations- und Mitteilungspflichten.[422]

Art.12 DS-GVO

Artikel 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

(2) Der Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 22. In den in Artikel 11 Absatz 2 genannten Fällen darf sich der Verantwortliche nur dann weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte gemäß den Artikeln 15 bis 22 tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren.

(3) Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Stellt die

422 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Seite.226, Rn. 1.

betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

(4) Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(5) Informationen gemäß den Artikeln 13 und 14 sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 15 bis 22 und Artikel 34 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

(6) Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß den Artikeln 15 bis 21 stellt, so kann er unbeschadet des Artikels 11 zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

(7) Die Informationen, die den betroffenen Personen gemäß den Artikeln 13 und 14 bereitzustellen sind, können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Werden die Bildsymbole in elektronischer Form dargestellt, müssen sie maschinenlesbar sein.

(8) Der Kommission wird die Befugnis übertragen, gemäß Artikel 92 delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung standardisierter Bildsymbole zu erlassen.[423]

Art. 12 wird durch die **Erwägungsgründe** 58, 59, 60, 73 näher erläutert. Art. 12 DS-GVO ist der „vor die Klammer" gezogene allgemeine Teil der Anforderungen an den Verantwortlichen bei der Erfüllung der Rechte der Betroffenen nach Art. 13 bis 22 sowie Art. 34 DS-GVO und ist daher bei der Anwendung dieser Regelungen zu berücksichtigen. Art. 12 stellt aufgrund der **hohen Bedeutung** der Transparenz für die tatsächliche Wahrnehmung der Rechte der betroffenen Personen eine der zentralen Regelungen der DS-GVO dar.[424]

Mithin regelt Art. 12 DS-GVO vor allem die Art und Weise bzw. die Verfahren, wie die einzelnen **Betroffenenrechte** zu erfüllen sind, so z.B. wie betroffene Personen über die Verarbeitung ihrer Daten zu informieren sind.[425]

Nach Abs. 1 muss die **Datenverarbeitungsinformation** der **betroffenen Person präzise**, **transparent**, **verständlich**, in **leichter Form** und in **klarer und einfacher Sprach**e erfolgen.[426]

3.13.1 Präzision

Präzise ist die Information, wenn sie einen hinreichenden Grad an Genauigkeit aufweist. Die Information darf also wesentliche Aspekte der Datenverarbeitung nicht auslassen. Eine abschließende Darstellung wird jedoch jedenfalls dann nicht zu fordern sein, wenn hierdurch die Verständlichkeit nicht mehr gewährleistet werden kann. Vielmehr werden die darzustellenden Informationen auf ihren für die betroffene Person relevanten Kern zu reduzieren sein. Insoweit steht die Anforderung der „**präzisen**" Information unter einem einschränkenden Vorbehalt der Verständlichkeit sowie klarer und einfacher Sprache. [427]

---

423 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art.12 DSGVO.

424 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Seite. 378, Rn. 1 Zweck der Vorschrift.

425 *Moos* (Hrsg.), Datennutzungs- und Datenschutzverträge, Seite 142, Rn. 7.

426 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Seite.227, Rn. 5.

427 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 17778 von 87533.

3.13.2 Verständlichkeit

Verständlichkeit erfordert hingegen, dass die Information für den jeweiligen Adressatenkreis aus sich heraus nachvollziehbar und ohne großen oder zusätzlichen Aufwand erfassbar ist. Dies kann einerseits Erläuterungen erforderlich machen, setzt aber auch und insbesondere voraus, dass nicht so viele kleinteilige Informationen und Erläuterungen gegeben werden, dass das Verständnis aufgrund der Informationsfülle wieder erschwert wird. Vielmehr muss die Darstellung so gewählt sein, dass der Inhalt klar und nachvollziehbar wird. Es kommt für die Verständlichkeit daher nicht auf eine umfassende Information an, sondern darauf, der Information die Komplexität zu nehmen und sie so für den Adressaten leichter fassbar zu machen.[428]

3.13.3 Transparenz

Transparenz ist ein Überbegriff für die Gesamtgestaltung und setzt voraus, dass der Inhalt an sich erkennbar ist und die wesentlichen Aussagen nicht verschleiert werden. Auch bei diesem Merkmal geht es letztlich um eine Gestaltung der Information, die diese durchschaubar und damit nachvollziehbar macht und die die wesentlichen Aussagen deutlich zu Tage treten lässt.[429]

Manche Kommentare führen die Begriffe Präzise und transparent gemeinsam aus, um einen Zusammenhang sinngemäß erläutert zu erhalten. Die Formulierung meint in diesem Zusammenhang, dass die Informationen kurz und knapp zur Verfügung gestellt werden müssen, um Informationsermüdung zu vermeiden.[430]

3.13.4 Leicht zugängliche Form

Die Form der Informationen und Mitteilungen muss leicht zugänglich ausgestaltet sein.[431] Dieses bedeutet, dass die Information für die betroffene Person ohne großen Aufwand verfügbar sein muss und sie nicht erst gesucht werden muss. [432]

---

428 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 17778 von 87533.

429 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 17778 von 87533.

430 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Seite 381, Rn. 10 Präzise und Transparent.

431 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Seite. 163, Rn. 32, Satz 1.

432 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Seite. 228, Rn. 9.

Leicht zugänglich ist die Information, wenn der Empfänger die Mitteilung selbst sowie ihren Inhalt mit den ihm zur Verfügung stehenden Mitteln erreichen kann, ohne dass zusätzliche Hürden errichtet werden. Dabei ist auch die Barrierefreiheit des Zugangs zu berücksichtigen, sowohl hinsichtlich verwendeter Dateiformate als auch bei farblichen Gestaltungen. Die Information darf zudem nicht verdeckt platziert werden. Vielmehr sollte für die betroffene Person sofort ersichtlich sein, wo die erforderlichen Informationen aufzufinden sind. Dies umfasst, insbesondere im Internet, eine aussagekräftige Benennung der Dokumente, in denen die Informationen enthalten sind, beispielsweise der Datenschutzerklärung oder der Allgemeinen Geschäftsbedingungen. Ein Link zu diesen Dokumenten sollte deutlich sichtbar und unter einem allgemein geläufigen Begriff (wie z.B. „Datenschutzhinweis“) auf der Website erscheinen. Im App-Bereich sollten hingegen bereits vor dem Download alle erforderlichen Informationen bereitgestellt werden. Sobald die App installiert ist, sollten die Informationen nie mehr als „zwei Klicks entfernt“ sein. Bei eingeschränkten Darstellungsmöglichkeiten, insbesondere bei mobilen Endgeräten und „embedded systems“, werden hinreichend klare und übliche Piktogramme jedoch ebenfalls ausreichend sein. Werden die Informationen schriftlich übermittelt, so umfasst dies in erster Linie die physische Zugänglichkeit und Lesbarkeit. Maßgeblich ist dabei der Gesamteindruck. So wird etwa allein eine vergleichsweise kleine Schrift je nach angesprochenen Verkehrskreisen nicht zwingend dazu führen, dass keine leichte Zugänglichkeit vorliegt.[433]

3.13.5 Klare und einfache Sprache

Auch wenn die Überschrift das Thema deutlich ausführt, so kann dieses doch zu stärkerer Verwirrung und Missverständnis führen als vorerst gedacht. Voraussetzung für klare und einfache Sprache ist, dass die Information so einfach wie möglich präsentiert wird und komplexe Sätze und Sprachkonstruktionen vermieden werden.[434] Dies erfordert eine eindeutige, soweit möglich nicht interpretationsoffene Formulierung. Auf relativierende und interpretationsoffene Begriffe wie „kann“, „könnte“, „dürfte“, „einige“, „oft“, „möglich“ **sollte** daher verzichtet werden. Vielmehr muss die betroffene Person absehen können, unter welchen Umständen welche Daten zu welchen Zwecken über sie

433 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 17778 von 87533, Rn. 28Rn.28..

434 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Seite. 382. Rn. 12, Satz 1.

verarbeitet werden. Einfachheit setzt zudem die Verwendung allgemein gebräuchlicher Worte und kurzer Sätze, deren Satzbau und Wortwahl verständlich sind, voraus. Fachbegriffe müssen je nach Adressatenkreis ggf. erläutert werden, beispielsweise durch weiterführende Links zu ausführlichen Erklärungen.[435] Sofern personenbezogene Daten über Kinder verarbeitet werden, muss der Verantwortliche dies gemäß Art. 12 Abs. 1 Satz 1, 2. Hs. DS-GVO im Rahmen der Transparenzanforderungen besonders berücksichtigen. Für den Begriff des Kindes i.S.d. DS-GVO kann auf Art. 8 DS-GVO verwiesen werden.[436]

Erwägungsgrund 58 spricht davon, dass immer dann, wenn sich „die Verarbeitung an Kinder richtet, … aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer dergestalt einfachen und klaren Sprache erfolgen sollten, dass ein Kind sie verstehen kann“ Auch hier wird die begleitende Verwendung von Bildsymbolen nach Abs. 7 eine besondere Rolle spielen.[437]

Erwägungsgrund 58:

Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente verwendet werden. Diese Information könnte in elektronischer Form bereitgestellt werden, beispielsweise auf einer Website, wenn sie für die Öffentlichkeit bestimmt ist. Dies gilt insbesondere für Situationen, wo die große Zahl der Beteiligten und die Komplexität der dazu benötigten Technik es der betroffenen Person schwer machen, zu erkennen und nachzuvollziehen, ob, von wem und zu welchem Zweck sie betreffende personenbezogene Daten erfasst werden, wie etwa bei der Werbung im Internet. **Wenn sich die Verarbeitung an Kinder richtet, sollten aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann.[438]**

---

435 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 17831 von 87533, Rn. 29.
436 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Seite 382, Rn. 13.
437 *J. Philipp Albrecht,* Datenschutzrecht, Seite. 622, Rn. 16.
438 STANDPUNKT (EU) Nr. 6/2016 DES RATES IN ERSTER LESUNG vom 2016, Erwägungsgrund 58.

3.13.6 Erleichterung der Rechteausübung (Art. 12, 15 - 22 DS-GVO)

Gemäß Art. 12 Abs. 2 Satz1 DS-GVO muss der Verantwortliche der betroffenen Person die Ausübung ihrer Rechte gemäß den Art. 15 - 22 DS-GVO erleichtern. Hiervon ist nicht lediglich ein Verbot der Erschwerung der Rechtsausübung erfasst. Vielmehr muss der Verantwortliche seine internen Prozesse so gestalten, dass die Rechteausübung möglichst einfach gemacht wird. Hierzu zählen u.a. elektronische Formulare und spezifische Anwendungen sowie gegeben falls Fernzugänge zu Daten.[439]

3.13.7 Unentgeltlichkeit

Im Unterschied zur bisherigen Rechtslage muss die Information des Betroffenen bzw. die Versendung von Mitteilungen an diesen nunmehr grundsätzlich unentgeltlich erfolgen. Bisher war es möglich, die tatsächlich entstandenen Kosten von dem Betroffenen einzufordern, auch wenn von dieser Möglichkeit häufig kein Gebrauch gemacht wurde.[440]

Allerdings sieht Abs. 5 von diesem Grundsatz in S. 2 Ausnahmen vor, um **missbräuchliche** und **leichtfertig** gestellte **Anträge** bereits von vornherein zu **unterbinden**.[441] Insofern ist die Ausnahme nur dann einschlägig, wenn das in Rede stehende Betroffenenrecht einen Antrag voraussetzt.[442]

Abs. 5 S. 2 eröffnet dem Verantwortlichen im Falle exzessiver oder offenkundig unbegründeter Anträge die Möglichkeit ein angemessenes Entgelt zu verlangen oder das Tätigwerden gänzlich zu verweigern.[443]

3.13.8 Zweifel an der Identität

Abs. 6 regelt den Fall, dass begründete Zweifel des Verantwortlichen an der Identität des Antragstellers bestehen. Zweifel an der Identität setzen voraus, dass die vorhandenen Daten auf eine bestimmte Identität hindeuten und somit eine Identifizierung grundsätzlich möglich ist, aber nach den Umständen Zweifel daran bestehen, ob der Antragsteller tatsächlich die als Betroffener identifizierte Person ist. Der Verantwortliche hat seine

---

439 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG KommentarErleichterung der Rechteausübung.
440 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Position 18049 von 87533, Rn. 59.
441 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Art. 12, Rn. 66 DSGVO.
442 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, Bäcker, S. 346, Rn. 30 (Art. 12 DSGVO).
443 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 18049 von 87533, Rn. 61.

Zweifel einzelfallbezogen darzulegen. Hintergrund der Regelung ist, dass die Informationen nur denjenigen zur Verfügung gestellt werden sollen, die auch tatsächlich durch die Datenverarbeitung betroffen sind. Eine routinemäßige Identitätsprüfung kann jedoch nicht auf Abs. 6 gestützt werden.[444]

In Betracht kommt bspw. die Vereinbarung einer Sicherheitsfrage oder die telefonische Abfrage von Kundendetails wie Geburtsdatum oder Mobilfunknummer, sofern diese Information beim Verantwortlichen bereits vorliegen. **Erwägungsgrund 57** sieht das Einloggen und Bestätigen der Anfrage in einem Kundenportal vor.[445]

Die Erforderlichkeit von Personalausweiskopien bedarf gesonderter Prüfung. Ggf. genügt bereits die Vorlage des Ausweises und ein entsprechender Vermerk (z.B.: „Personalausweis hat vorgelegen").

Laut **BayLDA** soll auf die Anforderung von Ausweiskopien verzichtet werden, wenn z.B. ein Auskunftsverlangen in unmittelbarem zeitlichem Zusammenhang (bis zu vier Wochen) mit einer Benachrichtigung steht, oder auch bei reinen Negativauskünften. Das BMI hat mit Schreiben vom 24.03.2016 weitere Voraussetzungen kommuniziert.

- Die Kopie darf ausschließlich zu Identifizierungszwecken verwendet werden
- Die Kopie muss als solche erkennbar sein.
- Daten, die nicht zur Identifizierung benötigt werden, können und sollen von den Betroffenen auf der Kopie geschwärzt werden. Dies gilt insbesondere für die auf dem Ausweis aufgedruckte Zugangs- und Seriennummer. Die Betroffenen auf die Möglichkeit und Notwendigkeit der Schwärzung hinzuweisen.
- Die Kopie ist vom Empfänger unverzüglich zu vernichten, sobald der mit der Kopie verfolgte Zweck erreicht ist.[446]

3.14 Verhaltensregeln und Zertifizierung (Art. 40 DS-GVO)

Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der

444 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, Bäcker, S. 347, Rn. 35 (Art. 12 DSGVO).
445 *Gola u. a.* (Hrsg.), Datenschutz-Grundverordnung, Seite. 326, Rn. 42.
446 *Gola u. a.* (Hrsg.), Datenschutz-Grundverordnung, Seite. 326, Rn. 43.

einzelnen Verarbeitungsbereiche und der besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen. Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, können Verhaltensregeln ausarbeiten oder ändern oder erweitern, mit denen die Anwendung dieser Verordnung beispielsweise zu dem Folgenden präzisiert wird:

a. faire und transparente Verarbeitung;
b. die berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen;
c. Erhebung personenbezogener Daten;
d. Pseudonymisierung personenbezogener Daten;
e. Unterrichtung der Öffentlichkeit der betroffenen Personen;
f. Ausübung der Rechte betroffener Personen;[447]
g. Unterrichtung und Schutz von Kindern und Art und Weise, in der die Einwilligung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist;
h. die Maßnahmen und Verfahren gemäß den Artikeln 24 und 25 und die Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel 32;
i. die Meldung von Verletzungen des Schutzes personenbezogener Daten an Aufsichtsbehörden und die Benachrichtigung der betroffenen Person von solchen Verletzungen des Schutzes personenbezogener Daten;
j. die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen oder
k. außergerichtliche Verfahren und sonstige Streitbeilegungsverfahren zur Beilegung von Streitigkeiten zwischen Verantwortlichen und betroffenen Personen im Zusammenhang mit der Verarbeitung, unbeschadet der Rechte betroffener Personen gemäß den Artikeln 77 und 79.[448]

447 *Klinger & Reicher Rechtstext Verlag,* EU-Datenschutz-Grundverordnung DSGVO, 28.07.2019, Verhaltensregeln und Zertifizierung, Position, 1013 von 2143, Abschnitt. 5.
448 *Klinger & Reicher Rechtstext Verlag,* EU-Datenschutz-Grundverordnung DSGVO, 28.07.2019, Verhaltensregeln und Zertifizierung, Position, 1013 von 2143, Abschnitt. 5.

Zusätzlich zur Einhaltung durch die unter diese Verordnung fallenden Verantwortlichen oder Auftragsverarbeiter können Verhaltensregeln, die gemäß Abs. 5 des vorliegenden Artikels genehmigt wurden und gemäß Absatz 9 des vorliegenden Artikels allgemeine Gültigkeit besitzen. Hierzu zählen ebenfalls Verantwortliche oder Auftragsverarbeiter, die gemäß Art. 3 nicht unter diese Verordnung fallen.

Diese Verantwortlichen oder Auftragsverarbeiter gehen mittels vertraglicher oder sonstiger rechtlich bindender Instrumente die verbindliche und durchsetzbare Verpflichtung ein, die geeigneten Garantien anzuwenden, auch im Hinblick auf die Rechte der betroffenen Personen. Die Verhaltensregeln gemäß Abs. 2 des vorliegenden Artikels müssen Verfahren vorsehen, die es der in Art. 41 Absatz 1 genannten Stelle ermöglichen, die obligatorische Überwachung der Einhaltung ihrer Bestimmungen durch die Verantwortlichen oder die Auftragsverarbeiter, die sich zur Anwendung der Verhaltensregeln verpflichten, vorzunehmen, unbeschadet der Aufgaben und Befugnisse der Aufsichtsbehörde, die nach Artikel 55 oder 56 zuständig ist.

Verbände und andere Vereinigungen gemäß Absatz 2 des vorliegenden Artikels, die beabsichtigen, Verhaltensregeln auszuarbeiten oder bestehende Verhaltensregeln zu ändern oder zu erweitern, legen den Entwurf der Verhaltensregeln bzw. den Entwurf zu deren Änderung oder Erweiterung der Aufsichtsbehörde vor, die nach Art. 55 zuständig ist.

Die Aufsichtsbehörde gibt eine Stellungnahme darüber ab, ob der Entwurf der Verhaltensregeln bzw. der Entwurf zu deren Änderung oder Erweiterung mit dieser Verordnung vereinbar ist und genehmigt diesen Entwurf der Verhaltensregeln bzw. den Entwurf zu deren Änderung oder Erweiterung, wenn sie der Auffassung ist, dass er ausreichende Garantien bietet. Wird durch die Stellungnahme nach Abs. 5 der Entwurf der Verhaltensregeln bzw. der Entwurf zu deren Änderung oder Erweiterung genehmigt und beziehen sich die betreffenden Verhaltensregeln nicht auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so nimmt die Aufsichtsbehörde die Verhaltensregeln in ein Verzeichnis auf und veröffentlicht diese. Bezieht sich der Entwurf der Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so legt die nach Art. 55 zuständige Aufsichtsbehörde, bevor sie den Entwurf der Verhaltensregeln bzw. den Entwurf zu deren Änderung oder Erweiterung genehmigt, ihn nach dem Verfahren gemäß Art. 63 dem Ausschuss vor, der zu der Frage Stellung nimmt.

Wird durch die Stellungnahme nach Abs. 7 bestätigt, dass der Entwurf der Verhaltensregeln bzw. der Entwurf zu deren Änderung oder Erweiterung mit dieser Verordnung vereinbar ist oder — im Fall nach Absatz 3 — geeignete Garantien vorsieht, so übermittelt der Ausschuss seine Stellungnahme der Kommission. Die Kommission kann im Wege von Durchführungsrechtsakten beschließen, dass die ihr gemäß Abs. 8 übermittelten genehmigten Verhaltensregeln bzw. deren genehmigte Änderung oder Erweiterung allgemeine Gültigkeit in der Union besitzen. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Art. 93 Abs. 2 erlassen. Die Kommission trägt dafür Sorge, dass die genehmigten Verhaltensregeln, denen gemäß Absatz 9 allgemeine Gültigkeit zuerkannt wurde, in geeigneter Weise veröffentlicht werden. Der Ausschuss nimmt alle genehmigten Verhaltensregeln bzw. deren genehmigte Änderungen oder Erweiterungen in ein Register auf und veröffentlicht sie in geeigneter Weise.[449]

Die Verhaltensregeln werden von den nationalen Aufsichtsbehörden und bei unionsweiten Verarbeitungen nach Beteiligung des Europäische Datenschutzausschusses genehmigt, Art. 40 Abs. 5 und 7 DS-GVO. Die Kommission kann Verhaltensregeln für allgemein gültig erklären, so dass diese dann als geeignete Garantien Datenverarbeitung in Drittländern ermöglicht, Art. 40 Abs. 3 und 9 DS-GVO.

Neben den Aufsichtsbehörden überwachen private Stellen, dass Datenverarbeiter die Verhaltensregeln einhalten, Art. 41 Abs. 1 DS-GVO. Die privaten Überwachungsstellen müssen sich dazu zuvor von den Aufsichtsbehörden akkreditieren lassen.[450] Das Fördern ist definiert als das Schaffen eines geeigneten Umfelds für die Entwicklung der Verhaltensregeln zu einem effektiven Werkzeug für die Kontrolle zur Einhaltung des Datenschutzes.[451]

449 *Klinger & Reicher Rechtstext Verlag,* EU-Datenschutz-Grundverordnung DSGVO, 28.07.2019, Art. 40 DSGVO, Position. 1089 von 2143.

450 *J. Philipp Albrecht/Jotzo,* Das neue Datenschutzrecht der EU, 2017, Verhaltensregeln und Zertifizierung, S. 99, D, Rn. 29.

451 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Förderung von Verhaltensregeln (Abs. 1), Art. 40 DSGVO, S. 867, Rn. 11.

4 Rechtsbehelfe, Haftung und Sanktionen

Die europäische Datenschutzreform steht im Zeichen des digitalen Zeitalters. Daten sind zu einer Ware geworden, die tagtäglich an finanzieller Bedeutung gewinnt. Rasche technologische Entwicklungen und die Globalisierung haben den Datenschutz vor neue Herausforderungen gestellt. Das Ausmaß der Erhebung und des Austauschs personenbezogener Daten hat eindrucksvoll zugenommen. Dem europäischen digitalen Binnenmarkt steht das Recht auf informationelle Selbstbestimmung und das Bedürfnis eines unionsweiten wirksamen Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten als Gegenspieler gegenüber. Die Grundverordnung verfolgt den Zweck, der Harmonisierung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung sowie die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten. Dazu gehört auch, dass die konsequente Durchsetzung der DS-GVO sichergestellt wird. Art. 58 Abs. 2 DS-GVO sieht hierfür eine Reihe an Abhilfebefugnissen vor. Eine der zehn Maßnahmen ist es, eine Geldbuße gemäß Art. 83 DS-GVO zu verhängen, zusätzlich zu oder anstelle von den in Art. 58 Abs. 2 lit. a) -h) und j) DS-GVO genannten Maßnahmen.[452]

Die zahllosen Verstöße gegen das Datenschutzrecht im Alltag schwächen das Vertrauen der Bürger in den Grundrechtsschutz und lassen sie zögern, moderne IT-Systeme noch stärker zu nutzen. Daher forderte das Europäische Parlament schon früh im Gesetzgebungsverfahren, dass Verstöße mit „angemessenen, harten und abschreckenden Sanktionen einschließlich strafrechtlicher Sanktionen geahndet werden“ sollten. Die dazu nötigen Rechtsbehelfe der Betroffenen, die zivilrechtliche Haftung von Verantwortlichen und Auftragsverarbeitern und anderen Sanktionen regelt Kapitel VIII der DS-GVO.[453]

452 RDV - Recht auf Datenverarbeitung 2017 (RDV Recht auf Datenverarbeitung, Ausgabe 02/2017, S. 13 - 20).

453 *J. Philipp Albrecht/Jotzo,* Das neue Datenschutzrecht der EU, 2017, S. 121, A, Grundlagen, Abs. 1 Rn. 1.

Nach **ErwGr. 141** DS-GVO sollen Betroffene Verstöße gegen ihre Rechte aus der Verordnung mit der Beschwerde oder einem gerichtlichen Rechtsbehelf rügen können.[454]

Erwägungsgrund 141

Jede betroffene Person sollte das Recht haben, bei einer einzigen Aufsichtsbehörde insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts eine Beschwerde einzureichen und gemäß Artikel 47 der Charta einen **wirksamen** gerichtlichen **Rechtsbehelf** einzulegen, wenn sie sich in ihren Rechten gemäß dieser Verordnung verletzt sieht oder wenn die Aufsichtsbehörde auf eine Beschwerde hin nicht tätig wird, eine Beschwerde teilweise oder ganz abweist oder ablehnt oder nicht tätig wird, obwohl dies zum Schutz der Rechte der betroffenen Person notwendig ist. Die auf eine Beschwerde folgende Untersuchung sollte vorbehaltlich gerichtlicher Überprüfung so weit gehen, wie dies im Einzelfall angemessen ist. Die Aufsichtsbehörde sollte die betroffene Person innerhalb eines angemessenen Zeitraums über den Fortgang und die Ergebnisse der Beschwerde unterrichten. Sollten weitere Untersuchungen oder die Abstimmung mit einer anderen Aufsichtsbehörde erforderlich sein, sollte die betroffene Person über den Zwischenstand informiert werden. Jede Aufsichtsbehörde sollte Maßnahmen zur Erleichterung der Einreichung von Beschwerden treffen, wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.[455]

454 *J. Philipp Albrecht/Jotzo,* Das neue Datenschutzrecht der EU, 2017, S. 121, A. Grundlagen, Abs. 2 Rn. 2.

455 Amtsblatt der Europäischen Union 04.05.2016 (Erwägungsgrund 141).

4.1 Ausgangslage

Deutschland gehört zu den Mitgliedsstaaten in der Europäischen Union, in denen „**administrative sanction**“ Tradition hat. Gemäß § 1 Abs. 1 OWiG ist die **Ordnungswidrigkeit** eine mit Geldbuße bedrohte, tatbestandsmäßige, rechtswidrige und vorwerfbare Handlung. Von ihr zu unterscheiden ist die Straftat, die eine mit Geld- und oder Freiheitsstrafe bedrohte Handlung ist. Im Gegensatz zur Kriminalstrafe fehlt der Geldbuße ein Unwerturteil und der Ernst staatlichen Strafens. Die Geldbuße ist in erster Linie darauf gerichtet, eine bestimmte Ordnung durchzusetzen, die Geldbuße ist eine ernste Pflichtenmahnung des Betroffenen. Die **mit Geldbußen sanktionierten Verstöße** gegen das Bundesdatenschutzgesetz (BDSG) sind derzeit in § 43 Abs. 1 und 2 BDSG geregelt. § 43 Abs. 1 BDSG enthält Tatbestände, die gemäß § 43 Abs. 3 S. 1, 1. Halbsatz BDSG mit einem Bußgeld von bis zu 50.000 EUR geahndet werden können. In § 43 Abs. 2 BDSG werden schwere Verstöße aufgeführt, für die gemäß § 43 Abs. 3 S. 1, 2. Halbsatz BDSG ein Bußgeld von bis zu 300.000 EUR verhängt werden kann. Das geltende Verfahren kann gegen natürliche Personen, natürliche und juristische Personen im gemeinsamen Verfahren oder gegen die natürliche Person und die juristische Person als Nebenbeteiligte in getrennten Verfahren geführt werden. Das Ordnungswidrigkeitenverfahren ist im Gesetz über Ordnungswidrigkeiten (OWiG) geregelt und wird durch die in Bezug genommenen Vorschriften der StPO, GVG und JGG über § 46 Abs. 1 OWiG ergänzt. Die Einhaltung des BDSG wird zum einen durch die Verhängung von Bußgeldern und zum anderen durch die Anordnungs- und Untersagungsrechte der Aufsichtsbehörde gemäß § 38 Abs. 5 BDSG gewährleistet. [456]

456 RDV - Recht auf Datenverarbeitung 2017 (RDV Recht auf Datenverarbeitung, S. 14).

4.2 Neue Vorschrift

Das geltende Verfahren kann gegen natürliche Personen, natürliche und juristische Personen im gemeinsamen Verfahren oder gegen die natürliche Person und die juristische Person als Nebenbeteiligte in getrennten Verfahren geführt werden. Das Ordnungswidrigkeitenverfahren ist im Gesetz über Ordnungswidrigkeiten (OWiG)[457] geregelt und wird durch die in Bezug genommenen Vorschriften der StPO, GVG und JGG über § 46 Abs. 1 OWiG ergänzt. Die Einhaltung des BDSG wird zum einen durch die Verhängung von Bußgeldern und zum anderen durch die **Anordnungs- und Untersagungsrechte** der Aufsichtsbehörde gemäß § 38 Abs. 5 BDSG gewährleistet.[458]

4.3 Zweck der Vorschrift

Bei Art. 82 DS-GVO handelt es sich um europäisches Sonderdeliktsrecht. Damit erstreckt der europäische Gesetzgeber das Primat der DS-GVO[459] auch auf das Zivilrecht.[460]

Mit der DS-GVO hat sich der europäische Gesetzgeber nicht nur der Gestaltung des öffentlichen Verwaltungs- sowie des Ordnungswidrigkeiten- und Strafrechts im Rahmen des Datenschutzes angenommen, sondern darüber hinaus auch unmittelbar geltende zivilrechtliche Anspruchsgrundlagen geformt. Art. 82[461] gewährt dem Betroffenen einen eigenen zivilrechtlichen deliktischen Schadenersatzanspruch gegen Verantwortliche und Auftragsverarbeiter. Dieser geht über die gesetzliche Delikts- und Vertragshaftung sowie ferner die Vorläuferregelungen, nämlich die auf Art. 23 DSRL[462] basierenden §§ 7, 8 BDSG a.F.[463] hinaus. § 7 BDSG a.F. bleibt insoweit hinter Art. 82 zurück, als er wohl nur Vermögensschäden ausgleicht und einen engeren Kreis hinsichtlich des

457 Ordnungswidrigkeiten Gesetz, Ordnungswidrigkeitengesetz.
458 RDV - Recht auf Datenverarbeitung 2017 (RDV Recht auf Datenverarbeitung, S. 14, II).
459 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).
460 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Haftung und Recht auf Schadenersatz, S. 1202, Rn. 3.
461 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 82 DSGVO.
462 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, Art. 23 DSRL, a. F.
463 (§§ 7, 8 BDSG a.F.).

Anspruchsverpflichteten statuiert. Schadenersatz über Art. 82 kann nicht nur für materielle, sondern auch für immaterielle Schäden verlangt werden. Die Norm ist Ausdruck des primärrechtlichen Effektivitätsgebots aus Art. 4 Abs. 3 EUV[464], indem die Geltendmachung des Schadenersatzanspruches wirksam ausgestaltet wird und so dem Datenschutz zur Entfaltung verhilft.[465]

4.4 Haftung und Recht auf Schadenersatz (Artikel 82 DS-GVO)

1. Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.
2. Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.[466]
3. Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Abs. 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.
4. Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.
5. Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Abs. 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder

---

464 *Vedder/Heintschel von Heinegg* (Hrsg.), Europäisches Unionsrecht, Vertrag über die Arbeitsweise der Europäischen Union, Art. 4 Abs. 3 EUV.

465 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 70978 von 87533, Rn. 1.

466 *Vedder/Heintschel von Heinegg* (Hrsg.), Europäisches Unionsrecht.

Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Abs. 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.[467]

6. Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen, die nach den in Artikel 79 Abs. 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.[468]

4.4.1 Anspruchsgrundlage (Art. 82 Abs. 1 DS-GVO)

Nach Art. 82 Abs. 1 DS-GVO hat jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.[469]

Anspruchsberechtigt ist beim Schadenersatz nach Art. 82 Abs. 1 DS-GVO „jede Person". Der Kreis der Anspruchsberechtigten ist trotz dieser Festlegung noch umstritten.[470]

Seinem Wortlaut nach schützt Art. 82 Abs. 1 „**Personen**", ohne danach zu unterscheiden, ob es sich um natürliche Personen oder juristische Personen handelt oder ob die Ansprüche auf Schadenersatz nur den betroffenen Personen, also denjenigen zustehen, deren Daten verarbeitet werden.[471]

Dagegen spricht allerding die Systematik des Artikels. In Abs. 4 wird im Rahmen der gesamtschuldnerischen Haftung auf die betroffene Person abgestellt, was nur Sinn ergibt, wenn auch in Abs.1 bereits nur die betroffene Person umfasst sein soll. Diese Auslegung wird auch von Erwägungsgrund [472] 146 S. 6 und S. 8 gestützt, die von der „betroffenen

---

467 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 70929 von 87533.

468 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 70929 von 87533.

469 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Anspruchsgrundlage Art.82 Abs. 1, S. 1205, Rn. 13.

470 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Anspruchsberechtigte, S. 1205, Rn. 14.

471 *Däubler et al.,* EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, Haftung und Recht auf Schadenersatz, S. 768, Rn. 4, II. Geschütze Personen.

472 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 146.

Person“ sprechen. Eine betroffene Person meint nach Art. 4 Nr. 1 DS-GVO stets eine natürliche Person.[473]

Erwägungsgrund 146

Der Verantwortliche oder der Auftragsverarbeiter muss Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht, ersetzen. Der Verantwortliche oder der Auftragsverarbeiter sollte von seiner Haftung befreit werden, wenn er nachweist, dass er in keiner Weise für den Schaden verantwortlich ist. Der Begriff des Schadens sollte im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht. Dies gilt unbeschadet von Schadenersatzforderungen aufgrund von Verstößen gegen andere Vorschriften des Unionsrechts oder des Rechts der Mitgliedstaaten. Zu einer Verarbeitung, die mit der vorliegenden Verordnung nicht im Einklang steht, zählt auch eine Verarbeitung, die nicht mit den nach Maßgabe der vorliegenden Verordnung erlassenen delegierten Rechtsakten und Durchführungsrechtsakten und Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen der vorliegenden Verordnung im Einklang steht. Die betroffenen Personen sollten einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten. Sind Verantwortliche oder Auftragsverarbeiter an derselben Verarbeitung beteiligt, so sollte jeder Verantwortliche oder Auftragsverarbeiter für den gesamten Schaden haftbar gemacht werden. Werden sie jedoch nach Maßgabe des Rechts der Mitgliedstaaten zu demselben Verfahren hinzugezogen, so können sie im Verhältnis zu der Verantwortung anteilmäßig haftbar gemacht werden, die jeder Verantwortliche oder Auftragsverarbeiter für den durch die Verarbeitung entstandenen Schaden zu tragen hat, sofern sichergestellt ist, dass die betroffene Person einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhält. Jeder Verantwortliche oder Auftragsverarbeiter, der den vollen Schadenersatz geleistet hat, kann anschließend ein Rückgriffsverfahren gegen andere an derselben Verarbeitung beteiligte Verantwortliche oder Auftragsverarbeiter anstrengen.[474]

---

473 *J. Philipp Albrecht,* Datenschutzrecht, Datenschutzrecht, Haftung und Recht auf Schadenersatz, S. 1203, Nr. 2, Rn. 8.

474 STANDPUNKT (EU) Nr. 6/2016 DES RATES IN ERSTER LESUNG vom 2016, Erwägungsgrund 146.

4.4.2 Anspruchsgegner / Anspruchsberechtigter (Art. 82 Abs.1 DS-GVO)

Mögliche Anspruchsgegner des Schadenersatzanspruches sind gemäß Art. 82 Abs. 1 DS-GVO alle an der Verarbeitung beteiligten Verantwortlichen und Auftragsverarbeiter. Der Haftungsumfang der Auftragsverarbeiter ist allerdings durch Art. 82 Abs. 2 Satz 2 DS-GVO begrenzt.[475]

Andere beteiligten Personen wie ein betrieblicher Datenschutzbeauftragter oder ein Geschäftsführer kommen nicht in Betracht. Das schließt nicht aus, dass im Verhältnis zu ihnen andere Vorschriften eingreifen, die eine Schadensersatzpflicht auslösen können.[476]

Ausweislich des Wortlautes ist jede Person, der durch einen Verstoß gegen die DS-GVO ein Schaden entstanden ist, berechtigt, Schadensersatz zu verlangen. Als Personen kommen nur natürliche Personen in Betracht, die von der Datenverarbeitung betroffen sein müssen. Teilweise wird vertreten, auch Dritte in den Kreis der Anspruchsberechtigten aufzunehmen.[477]

4.4.3 Haftung (Art. 82 Abs. 2 DS-GVO)

Die DS-GVO schafft ein neues Haftungsregime für die Auftragsverarbeitung, welche durch eine nicht unerhebliche Eigenhaftung des Auftragsverarbeiters geprägt ist. Nicht nur treffen den Auftragsverarbeiter direkt mehr Pflichten unter der DS-GVO; ihm gegenüber können Betroffene gemäß Art. 79 DS-GVO nun auch selbst gerichtliche Rechtsbehelfe geltend machen und über Art. 82 Abs. 1 DS-GVO können jedermann („jede Person“) – also nicht nur betroffene Personen – Schadensersatzansprüche direkt gegen den Auftragsverarbeiter zustehen.[478]

Die Haftung des Verantwortlichen auf Schadenersatz setzt voraus, dass er gegen Vorschriften des DS-GVO verstoßen hat. Deren Bedeutung spielt keine Rolle; es kann sich um materiell-rechtliche Zulassungsvorschriften wie Art. 6 oder um Verfahrensvorschriften wie die Bestellung eines Datenschutzbeauftragten oder die

475 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Haftung und Recht auf Schadenersatz, S. 1206, Anspruchsgegner, Rn. 18.

476 *Däubler et al.,* EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, Haftung und Recht auf Schadenersatz, S. 770, Rn. 7.

477 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 71180 von 87533, Rn. 16.

478 *Moos/Schefzig/Arning* in, De Gruyter Praxishandbuch (Seite. 260, Rn. 54).

Dokumentation nach Art. 30 handeln. Die Haftung tritt für jeden noch so kleinen Verstoß ein, soweit er kausal für die Entstehung des Schadens war. Nicht erforderlich ist, dass die Vorschrift **gerade den Schutz der betroffenen Person bezweckte.**[479]

Die Regelung des Art. 82 Abs. 2 DS-GVO ist keine eigenständige Anspruchsgrundlage, sie dient der Konkretisierung des Haftungsumfangs der jeweiligen Anspruchsgegner.[480]

Art. 82 Abs. 2 S. 1 stellt klar, dass jeder, der an einem Verarbeitungsvorgang i.S.v. Art. 4 Nr. 2 beteiligt ist, der Haftung aus Art. 82 Abs. 1 unterfallen kann. Art. 82 Abs. 2 S. 2 statuiert für den Auftragsverarbeiter eine Haftung für den Fall, dass dieser speziell ihm zugewiesene Pflichten, die aus der DS-GVO entspringen, vernachlässigt oder die Weisungen des Verantwortlichen missachtet bzw. gegen diese gehandelt hat. Der Auftragsverarbeiter agiert als „verlängerter Arm" des für die Datenverarbeitung Verantwortlichen und hat keine Kompetenz, selbstständig Entscheidungen zu treffen. Diese Stellung im Rahmen der Datenverarbeitung rechtfertigt die gegenüber dem Verantwortlichen bestehende Privilegierung in Bezug auf die Haftungsfrage.[481]

Auch wenn die Sanktionen des Art. 83 DS-GVO als „drakonisch" bezeichnet werden, ist eine weitaus größere Weiterentwicklung für die Durchsetzung des Datenschutzrechts und die Überwindung des Durchsetzungsdefizits vom Schadenersatzanspruch des Art. 82 zu erwarten. Auf zivilrechtlicher Ebene wird ein Anspruch auf Schadenersatz bei Verstößen gegen die Verarbeitungspflichten der DS-GVO gewährt und wegen des lex specialis-Charakters eine Sperrwirkung gegenüber konkurrierenden Ansprüchen aus §§ 823 ff. BGB[482] entfaltet. Der Auftragsdatenverarbeiter hat nun auch immateriellen Schäden zu ersetzen, wenn er gegen seine Pflichten verstößt (vgl. hierzu Art. 82 II DS-GVO). Zuvor war nur Ersatz für materielle Schäden zu leisten (vgl. Art. 7 DSRL), die dem Betroffenen normalerweise jedoch nicht entstanden, womit der Anspruch gem. § 253 I BGB leer lief. Datenschutzverstöße können bei Unternehmen zu „Klagewellen" führen, denn dem Betroffenen wird ein Vorgehen aus zwei Gründen erleichtert: Zum einen sehen Art. 5

---

479 *Däubler et al.,* EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, Haftung und Recht auf Schadenersatz, S. 771, Rn. 10+11.

480 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Haftung und Recht auf Schadenersatz, S. 1220, Rn. 59.

481 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 71226 von 87533, Rn. 22.

482 Bürgerliches Gesetzbuch, BGB - Bürgerliches Gesetzbuch.

Abs. 2 und Art. 24 Abs. 1 Satz 1 DS-GVO eine „**Beweislastumkehr**“ zu Ungunsten datenverarbeitender Unternehmen vor. Zum anderen werden durch § 44 Abs. 1 BDSG, welcher der Durchführung von Art. 79 Abs. 2 DS-GVO dient, zwei besondere Gerichtsstände geschaffen, zwischen denen der Kläger gem. § 35 ZPO zusätzlich wählen kann. Zu vermuten ist, dass insb. die Klageerhebung am Gericht des Ortes, an dem der Betroffene seinen gewöhnlichen Aufenthaltsort hat (vgl. § 44 Abs. 1 Satz 2 BDSG), die Hemmschwelle zur Klageerhebung absenkt. Zudem ist es gestattet, an jedem Ort, an dem der Verantwortliche eine Niederlassung unterhält, ohne dass es auf die zusätzliche Voraussetzung eines Bezugs zu der Niederlassung nach § 21 I ZPO ankommt, Klage zu erheben. Es ist also damit zu rechnen, dass Unternehmen zukünftig im gesamten Bundesgebiet verklagt werden. Zur Bemessung des Schadensersatzes selbst wird auf die Rechtsprechung des EuGHs verwiesen, der die abschreckende Wirkung von zivilrechtlichen Sanktionen betont.[483]

4.4.4 Haftungsbefreiung (Art. 82 Abs. 3 DS-GVO)

Art. 82 Abs. 3 DS-GVO verankert eine widerlegbare Verschuldungsvermutung zulasten des Anspruchsgegners eines Schadensersatzanspruchs (zu den allgemeinen Verschuldensmaßstäben oben Rn. 40 f.). Ein in Anspruch genommener Beteiligter einer Datenverarbeitung muss zum Zwecke seiner Entlastung gemäß Art. 82 Abs. 3 DS-GVO nachweisen, dass er in keiner Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Die Verwendung des Adjektivs „verantwortlich“ – wie schon in Art. 23 Abs. 2 DSRL dürfte auf einer Ungenauigkeit der Übersetzung beruhen und nicht die datenschutzrechtliche Verantwortlichkeit i.S.v. Art. 4 Nr. 7 DS-GVO, sondern das Verschulden meinen. Schließlich wäre der Auftragsverarbeiter schon von der Gesetzeskonstruktion her nie in einem solchen Sinne „verantwortlich“.[484]

Art. 82 Abs. 3 erlaubt es dem Verantwortlichen oder dem Auftragsverarbeiter sich von der Haftung zu befreien. Voraussetzung dafür ist, dass er nachweist, dass er für den Verstoß gegen die Verordnung nicht verantwortlich ist. Da die DS-GVO den Verantwortlichen und den Auftragsverarbeiter zu umfangreicher Dokumentation

---

483 AD Legendum AL 1/2018, 1 (Recht in der Digitalen Realität, S. 22, II Zivilrechtliche Haftung).

484 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Haftungsbefreiung Art. 82 Abs. 3, S. 1223, Rn. 70.

verpflichten (siehe insbesondere die Rechenschaftspflicht aus Art. 5 Abs. 2, und die allgemeine **TOM**s (**T**echnisch **O**rganisatorische **M**aßnahmen) aus Art. 24, 25 und 32) müssen diese demnach die Rechtmäßigkeit der von ihnen durchgeführten Datenverarbeitung nachweisen. Der von der Verordnungswidrigkeit Betroffene bleibt aufgrund dieser Beweislastumkehr geschützt und muss nicht schwer aufdeckbare und ggfs. interne Vorgänge nachweisen, die die Verantwortlichkeit belegen.[485]

Der Nachweis der Nichtverantwortlichkeit bezieht sich auf die vollkommene Pflichtenerfüllung im Rahmen eines Datenverarbeitungsvorgangs durch den Verantwortlichen oder den Auftragsverarbeiter. Die Verantwortlichkeit bezieht sich nicht auf die Beteiligung an der Datenverarbeitung, da ansonsten auch eine ausufernde Nachweispflicht für die negative Tatsache einer „Nicht-Beteiligung“ am Datenverarbeitungsvorgang bestünde.[486]

Was zu einer Nichtverantwortlichkeit führen kann, ist davon abhängig, wie der Begriff der Verantwortlichkeit im Sinne des Schadensersatzanspruchs verstanden wird. Mit Verantwortlichkeit ist ein Verschulden im Sinne einer subjektiven Vorwerfbarkeit gemeint.[487]

Letztlich werden damit nach deutschem Recht die Kategorien Vorsatz und Fahrlässigkeit angesprochen. Eine Haftungsbefreiung kommt nur dann in Betracht, wenn der Verantwortliche „in keiner Weise“ Verantwortlichkeit für den Schaden hat und damit auch keine Fahrlässigkeit gegeben ist.[488]

Der Verantwortlichkeits- bzw. Verschuldensbegriff wird europarechtlich und nicht nach §276 Abs. 1 BGB ausgelegt.[489]

Nach Art. 83 Abs. 2 lit. b unterscheidet die DS-GVO zwischen Vorsatz und Fahrlässigkeit. Missachten Verantwortliche oder Auftragsverarbeiter bewusst, also

---

485 Beck'scher Online-Kommentar Datenschutzrecht, Rn. 18.

486 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Frenzel, Art. 82, Rn. 15 DSGVO.

487 Beck'scher Online-Kommentar Datenschutzrecht, Rn. 17.

488 *Gola u. a.* (Hrsg.), Datenschutz-Grundverordnung, Gola, S. 746, Art. 82, Rn. 18 DSGVO, vgl. ebenfalls Frenzel, S. 82, Rn. 6 DSGVO (Paal - Pauly).

489 [Der Titel "EuGH C-135/82" kann nicht dargestellt werden. Die Vorlage "Fußnote - Zeitschriftenaufsatz - (Standardvorlage)" beinhaltet nur Felder, welche bei diesem Titel leer sind.]

vorsätzlich, oder vorsätzlich, oder fahrlässig eine in der DS-GVO genannte Pflichten, trifft sie das Verschulden und sie haften gemäß Art. 82, da der Verantwortliche oder Auftragsverarbeiter nachweisen muss, dass er in keinerlei Hinsicht für den Umstand verantwortlich ist, umfasst der Haftungsmaßstab Vorsatz und alle Formen der Fahrlässigkeit, inklusive leichter Fahrlässigkeit.[490]

4.4.5 Gesamtschuldnerische Haftung (Art. 82 Abs. 4)

Sind mehrere Anspruchsverpflichtete für den entstandenen Schaden verantwortlich, so haften diese gesamtschuldnerisch. Zur Sicherstellung der Wirksamkeit des Schadenersatzanspruchs kann der Anspruchsberechtigte von jedem an der Verarbeitung Beteiligten den Ersatz des gesamten Schadens verlangen, ErwGr. 146 Satz. 7.[491]

Wenn mehr als ein Verantwortlicher oder Auftragsverarbeiter an dem Datenverarbeitungsvorgang beteiligt und ferner auch für den Verordnungsverstoß verantwortlich sind, haften sie im Außenverhältnis gegenüber dem Betroffenen gemeinsam als Gesamtschuldner.[492] Dafür spricht vor allem **Erwägungsgrund 146,** S. 6, nach dem jeder an einem Verfahren Beteiligte für den gesamten Schaden haftbar gemacht werden können soll. § 840 BGB ist insoweit nicht mehr relevant. Rechtsfolge ist, dass jeder für den Ersatz des gesamten Schadens nach Wahl des Anspruchsberechtigten beansprucht werden kann. Dies entspricht dem Effektivitätsgrundsatz des Europarechts. Auf eine Ausnahme von dem Konzept der Gesamtschuld weist **Erwägungsgrund 146** S. 8 jedoch hin: Demnach kann ein Anspruch gegen mehrere Verantwortliche – die sämtliche nach den prozessualen Regeln des Mitgliedslandes an einem einzigen Prozess beteiligt sind – direkt anteilig zugesprochen werden.[493]

4.4.6 Innenausgleich (Art. 82 Abs. 5 DS-GVO)

Art. 82 Abs. 5[494] ermöglicht einen Innenausgleich zwischen den Gesamtschuldnern. Im Innenverhältnis werden die einzelnen Verursachungsbeiträge berücksichtigt. Als

---

490 *Bäcker,* Datenschutz-Grundverordnung, Art. 82, Rn. 54.
491 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Haftung und Recht auf Schadenersatz, S. 1042, Rn. 20.
492 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, Nemitz, S. 1072, Rn. 22.
493 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Art. 82 Abs .4, Position 71280, Rn. 28.
494 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener

Maßstab für die Berechnung des Verantwortungsanteils gilt Art. 82 Abs. 2.[495] In prozessrechtlicher Hinsicht ist eine Streitverkündung sinnvoll.[496] In der Praxis werden insbesondere in den Fällen einer gemeinschaftlichen Verantwortung die nach Art. 26 abzuschließenden Verträge und die darin vorgenommene Aufteilung der Verantwortung eine Rolle spielen.[497]

Abs. 5 knüpft an Abs. 4 an und regelt als eigene Anspruchsgrundlage den Innenausgleich zwischen Verantwortlichen und/oder Auftragsverarbeitern. Sie geht § 426 BGB[498] vor. Erfüllt also ein Gesamtschuldner im Sinne von Abs. 4 den Anspruch des Anspruchsstellers, kann er im Innenverhältnis Ausgleich verlangen. Nach dem Sinn und Zweck der Norm gilt dies auch, wenn ein Verantwortlicher oder Auftragsverarbeiter einen höheren Anteil übernommen hat, als er im Innenverhältnis eigentlich tragen musste.[499]

Ein Auftragsverarbeiter haftet bereits im Außenverhältnis nur dann, wenn er einen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DS-GVO nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisung gehandelt hat. Nur unter dieser Bedingung haftet er im Innenverhältnis.[500]

4.4.7 Internationaler Gerichtsstand (Art. 82 Abs. 6 DS-GVO)

Der internationale Gerichtsstand für Schadenersatzklagen richtet sich gemäß Art. 82 Abs. 6 nach Art. 79 Abs. 2.

Nach Art. 79 Abs. 2 ist der Anspruch vor den Gerichten der Mitgliedsstaaten geltend zu machen. In Betracht kommet das Gericht des Mitgliedsstaats, in dem das in Anspruch

---

Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 82 Abs. 5 DSGVO.

495 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, Kreße, S. 1268, Rn. 23.

496 Beck'scher Online-Kommentar Datenschutzrecht, Quaas, Art. 82, Rn. 45, vgl. ebenfalls Kühling/Buchner - Berg, Art. 82, Rn. 62.

497 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Art. 82 Abs. 4, Position 71280, Rn. 30.

498 Bürgerliches Gesetzbuch, § 426 BGB.

499 *Kühling /Buchner/Bergt*, in: *Kühling / Buchner / Bergt Art. 82 Rn. 60; Lauel / Nink / Kremer, § 11 Rn. 14; Sydow / Kreße Art. 82 Rn. 23*.

500 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, Haftung und Recht auf Schadenersatz, S. 1268, Rn. 24.

genommene Unternehmen eine Niederlassung hat, oder das Gericht des Mitgliedstaats, in dem der Anspruchsberechtigte seinen Aufenthaltsort hat.[501]

Das konkret zuständige Gericht auf mitgliedsstaatlicher Ebene richtet sich nach den nationalen Zuständigkeitsvorschriften,[502] also in Deutschland nach den §§ 12 ff. ZPO[503] bezüglich der örtlichen und den § 23 Abs. 1 in Verbindung mit § 71 Abs. 1 GVG[504] bezüglich der sachlichen Zuständigkeit.[505]

4.4.8 Ergänzende nationale Schadenersatzansprüche (Art. 82 DS-GVO)

In Deutschland gelten neben Art. 82 DS-GVO aber weiterhin die allgemeinen deliktischen Schadensersatznormen. Insbesondere sind

- § 823 Abs. 1 BGB i.V.m. dem allgemeinen Persönlichkeitsrecht bzw. eingerichteten und ausgeübten Gewerbetrieb,
- § 823 Abs. 2 i.V.m. individualschützenden Normen der DS-GVO und des BDSG (wobei der Schutzcharakter jeder Norm einzeln zu bestimmen ist)[506] sowie §§ 824, 826, 831 BGB und
- Bei Amtspflichtverletzungen § 839 BGB i.V.m. Art. 34 GG. relevant.[507]

4.5 Rechtsgrundlage (Art. 83 DS-GVO)

Der erste Blick gilt den Vorschriften in Art. 83 DS-GVO. Hieraus ergibt sich, ob ein bestimmter Verstoß gegen die DS-GVO auch mit einem Bußgeld verfolgt werden kann. Das Verfahrensrecht wiederum ist nach Art. 83 Abs. 8 und 9 DS-GVO nationale Angelegenheit und von den jeweiligen Mitgliedsstaaten zu regeln.[508]

---

501 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Haftung und Recht auf Schadenersatz, S. 1043, Rn. 25.
502 *Gola u. a.* (Hrsg.), Datenschutz-Grundverordnung, Örtliche und sachliche Zuständigkeit, S. 748, Rn. 29.
503 ZPO 2020, ZPO - Zivilprozessordnung.
504 Gerichtsverfassungsgesetz vom 2020, GVG - Gerichtsverfassungsgesetz.
505 *J. Philipp Albrecht/Jotzo,* Das neue Datenschutzrecht der EU, 2017, Teil 8 Rn. 28.
506 Datenschutzrecht in der betrieblichen Praxis.
507 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Haftung und Recht auf Schadenersatz, S. 1232, Rn. 103.
508 Recht auf Datenverarbeitung, Maria Christina Rost 2017, DuD 08/2019, S. 491, 3.1 Rechtsgrundlagen, Abs. 1.

4.5.1 Bußgeldzumessung (Art. 83 Abs. 1 DS-GVO)

Für die Bußgeldzumessung bei Verstößen gegen die DS-GVO sind die Vorschriften Art. 83 Abs. 1 und 2 DS-GVO relevant. Hintergrundinformationen ergeben sich aus **Erwägungsgründen 148** und 150 Satz 2, 3, 4. Sofern das EDPB[509] gemäß Art. 70 lit. k DS-GVO Leitlinien erlässt, nehmen diese ebenfalls Einfluss auf die Bußgeldzumessung. Die Grundverordnung fordert, dass es für die Verhängung von Sanktionen einschließlich Geldbußen angemessene Verfahrensgarantien geben soll, die den allgemeinen Grundsätzen des Unionsrechts und der Charta, einschließlich des Rechts auf wirksamen Rechtschutz und ein faires Verfahren, entsprechen.[510]

Erwägungsgrund 148

Im Interesse einer konsequenteren Durchsetzung der Vorschriften dieser Verordnung sollten bei Verstößen gegen diese Verordnung zusätzlich zu den geeigneten Maßnahmen, die die Aufsichtsbehörde gemäß dieser Verordnung verhängt, oder an Stelle solcher Maßnahmen Sanktionen einschließlich Geldbußen verhängt werden. Im Falle eines geringfügigeren Verstoßes oder falls voraussichtlich eine zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde, kann anstelle einer Geldbuße eine Verwarnung erteilt werden. Folgendem sollte jedoch gebührend Rechnung getragen werden: der Art, Schwere und Dauer des Verstoßes, dem vorsätzlichen Charakter des Verstoßes, den Maßnahmen zur Minderung des entstandenen Schadens, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, der Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, der Einhaltung der gegen den Verantwortlichen oder Auftragsverarbeiter angeordneten Maßnahmen, der Einhaltung von Verhaltensregeln und jedem anderen erschwerenden oder mildernden Umstand. Für die Verhängung von Sanktionen einschließlich Geldbußen sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, entsprechen.[511]

---

509 EDPB = European Data Protection Board,

510 STANDPUNKT (EU) Nr. 6/2016 DES RATES IN ERSTER LESUNG vom 2016, S. Erwägungsgrund 149 Satz 4 DS-GVO.

511 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 148.

Erwägungsgrund 150

Um die verwaltungsrechtlichen Sanktionen bei Verstößen gegen diese Verordnung zu vereinheitlichen und ihnen mehr Wirkung zu verleihen, sollte jede Aufsichtsbehörde befugt sein, Geldbußen zu verhängen. In dieser Verordnung sollten die Verstöße sowie die Obergrenze der entsprechenden Geldbußen und die Kriterien für ihre Festsetzung genannt werden, wobei diese Geldbußen von der zuständigen Aufsichtsbehörde in jedem Einzelfall unter Berücksichtigung aller besonderen Umstände und insbesondere der Art, Schwere und Dauer des Verstoßes und seiner Folgen sowie der Maßnahmen, die ergriffen worden sind, um die Einhaltung der aus dieser Verordnung erwachsenden Verpflichtungen zu gewährleisten und die Folgen des Verstoßes abzuwenden oder abzumildern, festzusetzen sind. Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff "Unternehmen" im Sinne der Artikel 101 und 102 AEUV verstanden werden. Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die Aufsichtsbehörde bei der Erwägung des angemessenen Betrags für die Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen. Das Kohärenzverfahren kann auch genutzt werden, um eine kohärente Anwendung von Geldbußen zu fördern. Die Mitgliedstaaten sollten bestimmen können, ob und inwieweit gegen Behörden Geldbußen verhängt werden können. Auch wenn die Aufsichtsbehörden bereits Geldbußen verhängt oder eine Verwarnung erteilt haben, können sie ihre anderen Befugnisse ausüben oder andere Sanktionen nach Maßgabe dieser Verordnung verhängen.[512]

4.5.2 Zumessungskriterien (Art. 83. Abs. 2 DS-GVO)

Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 lit. a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

512 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 150.

- Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
- jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
- Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;
- etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
- Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
- Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
- Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
- Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;
- Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und
- jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.[513]

513 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 82 Abs. 2.

4.5.3 Einzelfallbezogene Kriterien (Art. 83 Abs. 2 DS-GVO)

Die Entscheidung, ob neben den sonst von Art. 58 Abs. 2 vorgesehenen Maßnahmen oder auch an deren Stelle (Art. 83 Abs. 2 S. 1) - eine Geldbuße verhängt wird und falls ja, in welcher Höhe, ist von der Aufsichtsbehörde nach den Umstanden des Einzelfalls zu treffen. Abs. 2 S. 2 listet eine Reihe von Gesichtspunkten (als Festsetzungs- und Zumessungskriterien) auf, die dabei jeweils „gebührend" zu berücksichtigen sind. Dieser (im Vergleich etwa zu § 17 Abs. 3 des deutschen OWiG[514] oder auch zu §. 46 Abs. 2 StGB recht detaillierte) Kriterienkatalog ist insofern nicht abschließend, als nach der Auffangklausel unter lit. k gegebenenfalls auch noch „jegliche anderen erschwerenden oder mildernden Umstande" einzubeziehen sind. Davon abgesehen ist es im Ergebnis offensichtlich nicht gelungen, die einzelnen Punkte des (im Verlauf der Entstehungsgeschichte mehrfach veränderten) Katalogs in sinnvoller Weise systematisch zu ordnen. Maßgeblich ist zunächst die sachliche und zeitliche Dimension des in Rede stehenden Verstoßes (lit. a) mit Blick auf den Umfang und den Zweck der davon betroffenen Datenverarbeitung. Das Gewicht des Verstoßes wird dabei auch von seinen Folgen bestimmt (wie viele Personen sind davon in welchem Ausmaß betroffen? - zur Bedeutung besonderer Datenkategorien siehe lit. g). Bei „geringfügigeren" Verstößen kann eine bloße Verwarnung ausreichen (vgl. **Erwägungsgrund 148**).[515]

Mit der Formulierung des Abs. 2 Satz 1, insbesondere der Formulierung »zusätzlich zu oder anstelle von« (»in addition to, or instead of«) wird unzweideutig bestimmt, dass Aufsichtsbehörden **keine Maßnahme nach Art. 58 Abs. 2 ergreifen können, ohne ein Bußgeld** zu **verhängen.** Damit haben Aufsichtsbehörden bei festgestellten Verstößen drei Optionen. Sie können zum einen darauf verzichten, tätig zu werden. Diese Option zu wählen, ist Aufsichtsbehörden schon aufgrund der Grundkonzeption der DS-GVO, die eindeutig in Richtung des Tätigwerdens der Aufsichtsbehörden zielt, erschwert. Auch kann aus **Erwägungsgrund 148 Satz 2** geschlossen werden, dass dies allenfalls den Fällen vorbehalten ist, in denen ein Verstoß durch juristische Personen noch nicht einmal den Grad der Geringfügigkeit erreicht hat oder im Falle eines Verstoßes durch eine natürliche Person eine Geldbuße eine unverhältnismäßige Belastung bewirken würde.

514 Gesetz über Ordnungswidrigkeiten, in: Gesetze im Internet,
515 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, Einzelplatzbezogene Kriterien, Art. 83 Abs. 2, S. 1277 Rn. 11 -12.

Daneben stehen den Aufsichtsbehörden bei festgestellten Verstößen gegen die DS-GVO nur noch die Optionen offen, lediglich ein Bußgeld zu verhängen, ohne eine der übrigen Abhilfemaßnahmen nach Art. 58 Abs. 2 zu ergreifen (**Bußgeld ohne Maßnahme nach Art. 58 Abs. 2**) oder neben einer solchen Maßnahme ein Bußgeld zu verhängen. (**Bußgeld plus Maßnahme nach Art. 58 Abs. 2**). Die Option, lediglich eine Maßnahme nach Art. 58 Abs. 2 zu ergreifen (Maßnahme nach Art. 58 Abs. 2 ohne Bußgeld) besteht damit nach dem Wortlaut des Verordnungstextes nicht. Dies muss als **Entscheidung des europäischen Gesetzgebers** hingenommen werden.[516]

4.5.4 Kriterienkatalog (Abs. 2 Satz 2)

Der Kriterienkatalog des Art. 83 Abs. 2 Satz 2 DS-GVO ist das Herzstück des Art. 83 DS-GVO. Der Kriterienkatalog des Art. 83 Abs. 2 Satz 2 DS-GVO definiert, welche Faktoren die Aufsichtsbehörde bei der Entscheidung, ob sie ein Bußgeld verhängen und wie hoch es sein soll, zu berücksichtigen haben diese Kriterien spiegelbildlich im Datenschutzmanagement besondere Bedeutung.[517]

Abs. 2 lit. a bis lit. k beinhalten eine **große Anzahl** an Umständen, die der Aufsichtsbehörde als Kriterien dabei dienen sollen, in welcher Höhe sie Geldbußen verhängen, Wie sich aus lit. k ergibt, ist die Liste in Abs. 2 nicht abschließend.[518]

4.5.4.1 Art. 83 Abs. 2 S.2 lit. a DS-GVO

Die Aufsichtsbehörde hat Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens ihrer Entscheidung zugrunde zu legen.[519]

4.5.4.2 Art. 83 Abs. 2 S. 2 lit. b DS-GVO

Bei der Bußgeldzumessung spielt außerdem eine Rolle, ob die Tat vorsätzlich oder fahrlässig begangen wurde.[520] Vorsätzliche Verstöße sind, so ist die Formulierung in lit.

---

516 *Däubler et al.,* EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, Allgemeine Bedingungen für die Verhängung von Geldbußen, S. 786, Rn. 5 Art. 83 Abs. 2.

517 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Allgemeine Bedingungen für die Verhängung von Geldbußen, Art. 83 Abs. 2 Satz 2 DSGVO, S. 1246 Rn. 33.

518 *J. Philipp Albrecht,* Datenschutzrecht, Art. 83 Rn. 22, Satz 1 - 3.

519 Recht auf Datenverarbeitung, Bußgeld im digitalen Zeitalter, Ausgabe 01/2017,S. 17, Art. 83 Abs. 2 lit a.

520 Recht auf Datenverarbeitung, Bußgeld im digitalen Zeitalter, Ausgabe 01/2017,S. 18, Art. 83 Abs. 2 lit b.

b zu verstehen, grundsätzlich schwerer zu gewichten als lediglich fahrlässiges Handeln bzw. Unterlassen.[521] Lit. b ermöglicht es, den Grad des Verschuldens beim Verantwortlichen oder Auftragsverarbeiter zu ermitteln. Es stellt sich automatisch die Frage, auf welche Person bei nicht-natürlichen Personen abzustellen ist.[522]

4.5.4.3 Art. 83 Abs. 2 S. 2 lit. c DS-GVO

Berücksichtigt werden jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens. Dem Verantwortlichen oder Auftragsverarbeiter sollte es daher ein Anliegen sein, Maßnahmen zu ergreifen und sie zu dokumentieren.[523] Dabei ist der Begriff des Schadens nicht ausschließlich auf einem Vermögensschaden zu beziehen.[524]

4.5.4.4 Art. 83 Abs. 2 S. 2 lit. d DS-GVO

In die Beurteilung fließt außerdem der Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 DS-GVO getroffenen technischen und organisatorischen Maßnahmen ein.[525]

Bemühungen des Verantwortlichen bzw. Auftragsverarbeiters, einen bei dritten Personen entstandenen (materiellen) Schaden möglichst gering zu halten (bzw. auszugleichen), sind nach lit. d mildern zu berücksichtigen (vgl. hierzu ebenfalls lit. f).[526]

Verantwortung vor dem Hintergrund technisch-organisatorischer Maßnahmen (lit. d). Ebenso soll bei der Bemessung der Höhe der Geldbuße und bei der Entscheidung über ihre Verhängung der Grad der Verantwortung des Verantwortlichen oder Auftragsverarbeiters anhand der technisch-organisatorischen Maßnahmen, die nach den Art. 25 und 32 getroffen werden. Es können also unterschiedlich hohe Bußgelder für eine fehlerhafte Datenverarbeitung je nach Verantwortung verhängt werden.[527]

---

521 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, Popp, S. 1278, Rn. 13 Satz 1.
522 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, Nemitz, S. 1085, Rn. 17.
523 Recht auf Datenverarbeitung, Bußgeld im digitalen Zeitalter, Ausgabe 01/2017,S. 18, Art. 83 Abs. 2 lit c.
524 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, Nemitz, S. 1085, Rn. 19, Art. 83 Abs. 2 Satz 2 lit. c DSGVO.
525 Recht auf Datenverarbeitung, Bußgeld im digitalen Zeitalter, Ausgabe 01/2017,S. 18, Art. 83 Abs. 2 lit d.
526 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, Art. 83 Allgemeine Bedingungen für die Verhängung von Geldbußen, S. 1278 Rn.14.
527 *J. Philipp Albrecht,* Datenschutzrecht, Allgemeine Bedingungen für die Verhängung von Geldbußen, Art. 83 Abs. 2 lit. d, S. 1217 Rn. 28.

4.5.4.5 Art. 83 Abs. 2 S.2 lit. e DS-GVO

Kommt es nach einem erstmaligen Verstoß im Anschluss zu ähnlich gelagerten weiteren Verstößen und / oder Verstößen mit einem vergleichbaren oder identischen Unrechtsgehalt, so deutet dies auf die fehlende Einsicht des Verantwortlichen oder Auftragsverarbeiters hin. Eine höhere Geldbuße als bei einem erstmaligen Verstoß ist die Folge des Verhaltens.[528]

Für die Entscheidung über das „Ob" und das „Wie" sind auch etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters zu berücksichtigen.[529]

Um Wiederholungstäter schärfer zu sanktionieren, ist zu würdigen, ob der Täter bereits zuvor gegen Datenschutzrecht verstoßen hat (Art. 83 Abs. 2 Satz 2 lit. e DS-GVO) oder Maßnahmen nach Art. 58 Abs. 2 in Bezug auf denselben Gegenstand nicht befolgt hat. Beide Kriterien unterliegen Einschränkungen. Die etwaigen früheren Verstöße müssen „einschlägig" sein, um zur Verhängung einer Geldbuße beizutragen. D.h. es müssen keine gleichartigen Vergehen in der Vergangenheit begangen worden sein, sondern eine Ähnlichkeit bei den Rechtsverstößen reicht dafür aus.[530]

4.5.4.6 Art. 83 Abs. 2 S. 2 lit. f DS-GVO

Für den Betroffenen rechnet es sich, mit der Aufsichtsbehörde von sich aus zusammenzuarbeiten. In die Bußgeldzumessung fließt der Umfang der Zusammenarbeit mit der Aufsichtsbehörde ein, der aufgewandt wurde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern. Um einen Anhaltspunkt dafür zu erhalten, was an dieser Stelle sachdienlich wäre, kann man u.a. im Kartellrecht im Zusammenhang mit der dortigen Bonusregelung nachsehen.[531] Dort gibt es mittlerweile eine umfangreiche Rechtsprechung zu den verschärfenden und mildernden Faktoren.[532]

---

528 *J. Philipp Albrecht,* Datenschutzrecht, Allgemeine Bedingungen für die Verhängung von Geldbußen, Art. 83 Abs. 2 lit. d, S. 1218 Rn. 29.

529 Recht auf Datenverarbeitung, Art. 83 Abs. 2 lit. e DSGVO, S.18.

530 *Bäcker,* Datenschutz-Grundverordnung, Bergt, S. 1039, Rn. 56, Art. 83 Abs. 2 Satz 2 lit. e DSGVO.

531 Winterstein/Ceyssens/Wessely, in: Groeben/Schwarze/Hatje, AEUV, 7. Auflage, nach Art, 101, Rn. 46 ff. und vor allem Rn. 86 ff., Art. 83 Abs. 2 lit. f, hrsg. von in Groeben/Schwarze/Hatje Winterstein/Ceyssens/Wessely (zit. als *Bearbeiter* in Art. 83 Abs. 2 lit. f).

532 Recht auf Datenverarbeitung, Art. 83 Abs. 2 Satz 2 lit. f, S. 18, Ausgabe 02/2017.

Die aktive Zusammenarbeit mit der Aufsichtsbehörde soll bußgeldmindernd berücksichtigt werden, weil hierdurch die Arbeit der Aufsichtsbehörde erleichtert wird. Hierzu gehört z.B. der Hinweis, dass die rechtswidrige Datenverarbeitung länger als von der Aufsichtsbehörde angenommen angedauert hat oder die Lieferung von Beweismaterial.[533]

Lit. f bezieht den Grad der Kooperation mit der Aufsichtsbehörde als ermessensleitende Erwägung in die Bußgeldverhängung ein. Explizit bezieht sich die DS-GVO auf die Zusammenarbeit bei der Krisenreaktion der Verarbeiter und Auftragsverarbeiter, also bei den Anstrengungen, die unternommen werden, »um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern« (»to remedy the infringement and mitigate the possible adverse effects of the infringement«). Daneben kann nach Art. 31 DS-GVO zumindest auf die Verweigerung der darüberhinausgehenden Kooperationen mit der Aufsichtsbehörde Auswirkungen haben. Sie stellt selbst einen Verstoß gegen die DS-GVO dar, sofern es sich um eine von der Aufsichtsbehörde erbetene (»on request«) Kooperation handelte.[534]

4.5.4.7 Art. 83 Abs. 2 S. 2 lit. g DS-GVO

Für die Bewertung des Einzelfalls spielt es zudem eine Rolle, welche Kategorien personenbezogener Daten von dem Verstoß betroffen sind.[535]

Berücksichtigt werden sollen auch die von dem Verstoß betroffenen Kategorien personenbezogener Daten. Verstöße bei der Verarbeitung besonders geschützter Daten können demnach höher geahndet werden als Verstöße bezüglich anderer Datenkategorien. Neben den in Art. 9 genannten Datenkategorien können auch andere besonders geschützte Daten in Betracht kommen. Werden beispielsweise keinerlei Maßnahmen getroffen, um bei der Verarbeitung von Daten über Kinder dies besonders zu schützen (vgl. hierzu Erwägungsgrund 38), kann dies bei der Bußgeldbemessung berücksichtigt werden.[536]

---

533 Beck'scher Online-Kommentar Datenschutzrecht, Holländer, Art. 83, Rn. 38.
534 *Däubler et al.,* EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, Allgemeine Bedingungen für die Verhängung von Geldbußen, Art. 83 Abs. 2 lit. f, S. 791 Rn. 16.
535 Recht auf Datenverarbeitung, Art. 83 Abs. 2. Satz 2 lit. g, Ausgabe 02/2017, S. 18.
536 *J. Philipp Albrecht,* Datenschutzrecht, Allgemeine Bedingungen für die Verhängung von Geldbußen, Art. 83 Abs. 2, lit. g, S. 1218 Rn. 31.

Erwägungsgrund 38

Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. Ein solcher besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen. Die Einwilligung des Trägers der elterlichen Verantwortung sollte im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein.[537]

Die Relevanz der jeweiligen Datenkategorie wird in lit. g noch einmal ausdrücklich hervorgehoben. Danach wird insbesondere erschwerend ins Gewicht fallen können, dass sich der in Rede stehender Verstoß auf Daten der in Art. 9 bezeichneter Art bezogen hat.[538]

4.5.4.8 Art. 83 Abs. 2 S. 2 lit. h DS-GVO

Die Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat, werden ebenfalls berücksichtigt.[539]

Das Kriterium in lit. h ließe sich durchaus unter die Zusammenarbeit mit den Aufsichtsbehörden (lit. f) subsummieren. Kooperation zwischen dem Verantwortlichen und der Aufsichtsbehörde kann auch derart Ausdruck finden, indem die gegen Datenschutzrecht verstoßende Person oder Stelle ihr Vergehen selbst bei der Aufsichtsbehörde notifiziert. Das kann eine entlastende Wirkung zugunsten des Verantwortlichen oder des Auftragsverarbeiters entfalten.[540]

---

537 Amtsblatt der Europäischen Union 04.05.2016 (Erwägungsgrund 38 DSGVO).
538 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, Allgemeine Bedingungen für die Verhängung von Geldbußen, Art. 83 Abs. 2, lit. g, S. 1278 Rn. 18, Satz 2.
539 Recht auf Datenverarbeitung, Art. 83 Abs. 2. Satz 2 lit h, Ausgabe 02/2017, S. 18.
540 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Art. 83 Abs.2 lit. h, Position 72260 von 87533, Rn. 48.

Die bloße Erfüllung der Meldepflicht nach Art. 33 Abs. 1 DS-GVO soll nach Ansicht der Aufsichtsbehörden kein mildernder Faktor sein.[541]

Eine überobligatorische umfassende Kooperation dürfte aber belohnt werden.[542] Ein Verantwortlicher bzw. Auftragsverarbeiter der mindestens fahrlässig keine Meldung an die Aufsichtsbehörde macht oder zumindest nicht alle Details des Verstoßes mitteilt, soll hingegen ein höheres Bußgeld erhalten.[543]

Hierzu sollten die Leitlinien des Ausschusses nach Art. 70 Abs. 1 lit. k konkrete Bewertungsmaßstäbe und Verfahrensweisen zur Verfügung stellen.[544]

4.5.4.9 Art. 83 Abs. 2 S. 2 lit. i DS-GVO

Relevant für die Beurteilung des Einzelfalls ist die Einhaltung der nach Artikel 58 Absatz 2 DS-GVO früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden. Mit anderen Worten: Hat die Aufsichtsbehörde hier bereits andere Maßnahmen angeordnet und wurden diese nicht eingehalten, wird dies voraussichtlich erschwerend Berücksichtigung in der Entscheidung der Aufsichtsbehörde finden.[545]

Nach Art. 83 Abs. 2 Satz 2 lit. i DS-GVO sind früher gegen den Verantwortlichen oder Auftragsverarbeiter in Bezug auf dieselbe Sache erteilte Weisungen zu berücksichtigen. Die Regelung sanktioniert im Rahmen von Art. 83 die mangelnde Befolgung dieser Weisungen.[546]

Es handelt sich hierbei nicht um eine Wiederholung des Kriteriums nach Art. 83 Abs. 2 Satz 2 lit. e DS-GVO. Vielmehr stellt Art. 83 Abs. 2 Satz 2 lit. i DS-GVO sicher, dass

---

541 *Datenschutzgruppe 29,* Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, WP 253, S. 16.

542 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, Rechtsbehelfe, Haftung und Sanktionen, S. 1086 Rn. 26 in Anlehnung an die Kronzeugenregelung der Kommission im Wettbewerbsrecht.

543 *Datenschutzgruppe 29,* Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, WP 253, S. 16.

544 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, Art. 83 Abs. 2 lit. h, S. 1087 Rn. 26, Satz 2.

545 Recht auf Datenverarbeitung, Art. 83 Abs. 2. Satz 2 lit i, Ausgabe 02/2017, S. 18.

546 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, Allgemeine Bedingungen für Geldbußen, Art. 83 Abs. 2 lit. i, S. 1087 Rn. 27.

auch die Umsetzung zuvor verhängter Maßnahmen im Rahmen desselben Gegenstands betrachtet wird.[547]

4.5.4.10 Art. 83 Abs. 2 S. 2 lit. j DS-GVO

Die Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 DS-GVO und von genehmigten Zertifizierungsverfahren nach Artikel 42 DS-GVO fließt ebenfalls in die Bußgeldzumessung mit ein. Dadurch wird die Durchführung solcher Maßnahmen für Unternehmen an Attraktivität gewinnen.[548]

Auch diese Bestimmung erklärt sich ohne weiteres von selbst. Sie zwingt die Verantwortlichen und Auftragsverarbeiter dazu, genehmigte Verhaltensregeln und genehmigte Zertifizierungsverfahren auch tatsächlich einzuhalten.[549]

So wie in lit. i ist gleichermaßen die Einhaltung der von Aufsichtsbehörden genehmigten Verhaltensregeln nach Art. 40 zu berücksichtigen bei der Verhängung von Bußgeldern. Analog ist die Einhaltung von Zertifizierungsverfahren nach Art. 42 zu würdigen, die auch durch die zuständige Aufsichtsbehörde genehmigt wurden oder alternativ von Seiten einer Zertifizierungsstelle nach Art. 43. Bei letztgenannter Stelle handelt es sich anders als bei einer Aufsichtsbehörde nicht um eine exekutive Einrichtung, gleichwohl siedelt sie auf unmittelbar anwendbarem Sekundärrecht. Diesem Umstand muss die Behörde bei Aussprache einer Geldbuße Rechnung tragen.[550]

Ebenso soll die Einhaltung oder die Missachtung von genehmigten Verhaltensregeln nach Art. 40, beispielsweise zur fairen und transparenten Verarbeitung (Abs. 2 lit. a) oder zur Ausübung der Rechte betroffener Personen (Abs. 2 lit. f), oder von genehmigten Zertifizierungsverfahren nach Art. 42 sich bei der Zumessung auswirken.

Dabei ist eine Auslegung in zwei verschiedene Richtungen denkbar. Einerseits kann davon ausgegangen werden, dass schon die Existenz von freiwilligen Verhaltensregeln an sich positiv zu betrachten ist und aus diesem Grund eine Missachtung dieser Regel und damit zugleich der Verordnung nicht so schwer wiegen soll, wie ein Verstoß nur

---

547 *Datenschutzgruppe 29,* Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, WP 253, S. 16.

548 Recht auf Datenverarbeitung, Art. 83 Abs. 2. Satz 2 lit j, Ausgabe 02/2017, S. 18.

549 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, Allgemeine Bedingungen für Geldbußen, Art. 83 Abs. 2 Satz 2 lit. j DSGVO, S. 1087 Rn. 28.

550 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Art. 83 Abs. 2 Satz 2, lit. j, Position 72262, Rn. 44.

gegen die Verordnung ohne die Existenz von Verhaltensregeln. Anderseits lässt sich argumentieren, dass ein Verstoß gegen Verhaltensregeln gravierender ist, als ein Verstoß nur gegen die Verordnung, da es sich bei den Verhaltensregeln um werbewirksame Maßnahmen handeln kann, die den betroffenen Personen zur Nutzung des Dienstes oder Angebots erst bewogen haben. Daher sollte die Missachtung von Verhaltensregeln sich ebenfalls bußgelderhöhend auswirken, wenn der Verantwortliche oder Auftragsverarbeiter mit den Verhaltensregeln geworben hat.[551]

4.5.4.11 Art. 83 Abs. 2 S. 2 lit. k DS-GVO

Außerdem fließen in die Bewertung jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall ein, wie z.B. unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.[552]

In lit. k des Abs. 2 hat der Verordnungsgeber eine Auffangregelung installiert. Diese erlaubt den bußgeldverhängenden Aufsichtsbehörden, „jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall“ berücksichtigen zu dürfen. Als Beispiel fügt er den durch den Verstoß erlangten wirtschaftlichen Vorteil an.[553]

Der Verweis auf die Berücksichtigung der unmittelbar oder mittelbar durch den Verstoß erlangten finanziellen Vorteile oder vermiedene Verluste wird hierfür lediglich als Beispiel genannt. Der finanzielle Vorteil aus einem Verstoß wird einem mathematischen Wert zu entsprechen haben. Dieser wiederum muss in einer konkreten Beziehung zu einem persönlichen Datum stehen. Die konkrete Berechnung eines Wertes, bezogen auf einen Datensatz über eine Person, kann bspw. anhand eines sozialen Netzwerks vorgenommen werden. Wird der Unternehmenswert des sozialen Netzwerks durch die Anzahl der Mitglieder des Netzwerkes geteilt, erhält man einen anzusetzenden Betrag.[554] [555]

---

551 *J. Philipp Albrecht,* Datenschutzrecht, Art. 83 Abs. 2 Satz 2, lit. j, S. 1218 Rn. 34.
552 Recht auf Datenverarbeitung, Art. 83 Abs. 2. Satz 2 lit. k, Ausgabe 02/2017, S. 18.
553 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Art. 83 Abs. 2 Satz 2 lit. k, Pos. 72262, Rn. 49.
554 *Däubler et al.,* EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, Allgemeine Bedingungen für die Verhängung von Geldbußen, Art. 83 Abs. 2 Satz 2, lit. k, S. 792 Rn. 21.
555 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, Nemitz, S. 1087, Rn. 29, Art. 83 DS-GVO.

4.5.5 Deckelung nach Art. 83 Abs. 3 DS-GVO

Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen der Verordnung, ist bei der Gesamtbemessung der Geldbuße Abs. 3 zu beachten. Die Formulierung des Abs. 3 lässt es in Anlehnung an nationale Regelungen naheliegen, den Fall, in dem eine Handlung mehrere Tatbestände verletzt, als Tateinheit zu bezeichnen. Zudem ist Abs. 3 bei Verstößen bei mehreren Verarbeitungsvorgängen, also der Fall von Tatmehrheit, einschlägig. Liegen die Voraussetzungen des Abs. 3 vor, ist nur eine Gesamtgeldbuße für sämtliche Tatbestände zu bilden. Nicht unerwähnt bleiben sollte, dass zu den Voraussetzungen des Abs. 3 ausdrücklich ein Verschuldensmoment gehört. Der Betrag der Gesamtgeldbuße als Rechtsfolge darf gem. Abs. 3 nicht den Betrag für den schwerwiegendsten Verstoß überschreiten.

Gleiche oder miteinander verbundene Verarbeitungsvorgänge (Abs. 3). Abs. 3 enthält eine Privilegierung für Verstöße gegen mehrere Bestimmungen der Verordnung im Fall gleicher oder miteinander verbundener Verarbeitungsvorgänge. Die Begriffe „gleich“ oder „miteinander verbunden“ sind in Abs. 3 nicht näher erläutert.[556]

Der Begriff miteinander verbundener Verarbeitungsvorgänge ist weder legal definiert noch wird er in der DS-GVO anderweitig verwendet. Nach dem Zweck des Abs. 3 ist der Begriff jedoch eng auszulegen, da sonst die abschreckende Wirkung des Art. 83 unterlaufen würde.[557]

4.5.6 Systematik der Bußgeldtatbestände (Art. 83 Abs. 4, 5 und 6 DS-GVO)

Die neuen, mit Bußgeldern sanktionierten Tatbestände sind in Art. 83 Abs. 4, 5 und 6 DS-GVO geregelt. Teilt man die Tatbestände nach ihrem Bußgeldrahmen auf, ergeben sich zwei Gruppen. Die erste Gruppe sind die Tatbestände in Art. 83 Abs. 4 DS-GVO. Ihre Verletzung kann mit einem Bußgeld bis zu 10 Mio. Euro sanktioniert werden. Der Höchstbetrag von 10 Mio. Euro kann überschritten werden, wenn ein Unternehmen im

556 *J. Philipp Albrecht,* Datenschutzrecht, Art. 83 Abs. 3 DSGVO, S. 1218 Rn. 36.
557 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, Allgemeine Bedingungen für Geldbußen, Art.83 Abs. 3, 2 Absatz, S. 1087 Rn. 31.

letzten Geschäftsjahr einen weltweiten Umsatz erzielt hat, von dem 2 % höher sind als der Höchstbetrag von 10 Mio. Euro.[558]

4.5.7 Bußgeldtatbestände (Art. 83 Abs. 5 und 6 DS-GVO)

Die zweite Gruppe sind die Bußgeldtatbestände nach Art. 83 Abs. 5 und 6 DS-GVO. Ihre Verletzung kann mit einem Bußgeld von bis zu 20 Mio. Euro geahndet werden bzw. mit Bußgeldern bis zu 4 % des weltweiten Jahresumsatzes eines Unternehmens. Art. 83 Abs. 4 und 5 DS-GVO sanktionieren Verpflichtungen, die sich aus der DS-GVO ergeben. Art. 83 Abs. 6 DS-GVO sanktioniert die Verstöße, die eine Missachtung einer Anweisung der Aufsichtsbehörde aus Artikel 58 Abs. 2 DS-GVO darstellen. Die in Art. 83 DS-GVO normierten Tatbestände reichen deutlich weiter als die bisherigen Bußgeldtatbestände nach § 43 BDSG. Der in Artikel 103 Abs. 2 GG enthaltene verfassungsrechtliche Bestimmtheitsgrundsatz enthält die Verpflichtung des Gesetzgebers, die Voraussetzungen der Strafbarkeit so konkret zu umschreiben, dass Tragweite und Anwendungsbereich der Straf- und Ordnungswidrigkeitentatbestände zu erkennen sind und sich durch Auslegung ermitteln lassen. In der Unbestimmtheit der Tatbestände liegen aus Unternehmenssicht erhebliche Haftungsrisiken.[559]

4.5.8 Adressaten der Bußgelder (Art. 83 Abs. 4 DS-GVO)

Potenzielle Adressaten der Bußgelder gemäß Art. 83 Abs. 4, 5 und 6 DS-GVO sind sowohl natürliche Personen als auch Unternehmen der primäre Adressatenkreis sind dabei „Verantwortliche, Auftragsverarbeiter sowie Überwachungs- und Zertifizierungsstellen.[560]

Sanktioniert werden nach Art. 83 Abs. 4 lit. a DS-GVO Verstöße gegen die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43 DS-GVO. Art. 83 Abs. 4 lit. b DS-GVO sanktioniert Verstöße gegen die Pflichten der Zertifizierungsstelle gem. Art. 42 und 43 DS-GVO. Nach Art. 83 Abs. 4 lit. c DS-

---

558 RDV - Recht auf Datenverarbeitung 2017 (RDV Recht aus Datenverarbeitung, S. 15, Abs. V); *Rost* Datenschutz Datensich 2019, 488.

559 Recht auf Datenverarbeitung, S. 15, Spalte 2.

560 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 83 Abs. 4 lit. b I.V.m. Art. 42, 43 DSGVO und Art. 83 Abs. 4 lit. c i.V.m. Art. 41 Abs. 4 DSGVO

GVO werden Verstöße gegen die Pflichten der Überwachungsstelle gemäß Artikel 41 Abs. 4 DS-GVO geahndet.[561]

Nach Abs. 4 lit. a sind Verstöße gegen die Pflichten der Verantwortlichen und der Auftragsverarbeiter gem. den Art. 8, 11, 25 bis 39, 42 und 43 bußgeldbewährt. So führt eine fehlerhafte Einwilligung von Minderjährigen i.S.d. Art. 8 oder eine Verletzung der Meldepflicht des Verantwortlichen nach Art. 33 zu einem Bußgeld in der Größenordnung von maximal 10 Millionen EUR bzw. 2 % des weltweiten Vorjahreskonzernumsatzes.[562]

Auch der Verstoß einer Zertifizierungsstelle gegen ihre Pflichten gem. den Art. 42 und 43 eröffnet den Bußgeldrahmen des Abs. 4. Danach sind die Zertifizierungsstellen verpflichtet, die entsprechend Art. 42 Abs. 5 für die Zertifizierung genehmigten Kriterien einzuhalten. Ein Verstoß gegen diese Pflicht dient als Anknüpfungstatbestand.[563]

Gemäß Art. 83 Abs. 4 DS-GVO werden für Verstöße gegen die folgenden Bestimmungen Geldbußen von bis zu EUR 10.000.000,00 oder im Fall eines Unternehmens von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des **vorangegangenen Geschäftsjahrs** verhängt, je nachdem, welcher der Beträge höher ist:[564]

a) Abs. 4 lit. a

Art. 83 Abs. 4 lit. a DS-GVO sanktioniert Verstöße gegen die folgenden Normen der DS-GVO:

- Art. 8: Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft
- Art. 11: Verarbeitung, für die eine Identifizierung des Betroffenen nicht erforderlich ist
- Art. 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- Art. 26: Gemeinsame Verantwortlichkeit

561 Recht auf Datenverarbeitung, S. 15, Nr. 1 Art. 83 Abs. 4.
562 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Tatbestände Art. 83 Abs. 4, Position 72464, Rn. 76.
563 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Tatbestände Art. 83 Abs. 4, Position 72464 von 87533, Rn. 77.
564 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, Sanktionen, 7.3.2 Gründe für Bußgelder und Bußgeldbeträge, S. 277, Abs. 2.

- Art. 27: Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern
- Art. 28: Auftragsverarbeitung
- Art. 29: Verarbeitung unter Aufsicht des Verantwortlichen oder des Auftragsverarbeiters
- Art. 30: Verzeichnis von Verarbeitungstätigkeiten
- Art. 31: Zusammenarbeit mit der Aufsichtsbehörde
- Art. 32: Sicherheit der Verarbeitung[565]
- Art. 33: Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde
- Art. 34: Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person
- Art. 35: Datenschutz-Folgeabschätzung
- Art. 36: Vorherige Konsultation
- Art. 37: Benennung eines Datenschutzbeauftragten
- Art. 38: Stellung des Datenschutzbeauftragten
- Art. 39: Aufgaben des Datenschutzbeauftragten
- Art. 42: Zertifizierung
- Art. 43: Zertifizierungsstellen[566]

b) Abs. 4 lit. b

- Zertifizierungsstellen unterliegen nach Art. 42 und 43 DS-GVO speziell auf sie zugeschnittenen Pflichten, deren Verletzung ebenfalls mit einem Bußgeld bedroht ist.[567]
- Auch der Verstoß einer Zertifizierungsstelle gegen ihre Pflichten gem. den Art. 42 und 43 eröffnet den Bußgeldrahmen des Abs. 4. Danach sind die Zertifizierungsstellen verpflichtet, die entsprechend Art. 42 Abs. 5 für die

565 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Bußgeldtatbestände (Abs. 4–6), Abs. 4 lit. a, S. 1265, Rn. 96.
566 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Bußgeldtatbestände (Abs. 4–6), Abs. 4 lit. a, S. 1265, Rn. 96.
567 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Bußgeldtatbestände (Abs. 4–6), Abs. 4 lit. b, S. 1265, Rn. 97.

Zertifizierung genehmigten Kriterien einzuhalten. Ein Verstoß gegen diese Pflicht dient als Anknüpfungstatbestand.[568]

- Abs. 5 droht für Verstöße gegen die dort genannten Vorschriften Geldbußen an, ohne dies auf die Pflichten bestimmter Personen zu beschränken. Die Sanktionsdrohung folgt mithin vollständig der Pflicht im Sachenrecht. Zu beachten ist insbes., dass als handelnde Person selbst zum Verantwortlichen wird, wer über die Zwecke und Mittel der Verarbeitung bestimmt, insbesondere Weisungswidrig personenbezogene Daten für sich selbst verarbeitet.[569]

4.5.9 Verstöße nach Art. 83 Abs. 5 DS-GVO

Verstöße gegen die in Art. 83 Abs. 5 aufgelisteten Pflichten werden als schwere Verstöße eingestuft. Ihr Bußgeldrahmen reicht bis zu 20 Mio. Euro. Hierunter fallen Verstöße gegen die Grundsätze der Verarbeitung einschließlich der Bedingungen für die Einwilligung gemäß den Artikeln 5, 6, 7 und 9 DS-GVO[570]. Verstöße gegen die Rechte der betroffenen Personen gemäß Artikel 12 bis 22 DS-GVO[571], Verstöße gegen die Pflichten im Rahmen der Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49 DS-GVO[572], die Nichtbefolgung aller Pflichten gemäß den Rechtsvorschriften der Mitgliedsstaaten, die im Rahmen des Kapitels IX der DS-GVO erlassen wurden[573], sowie die Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Abs. 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Abs. 1 DS-GVO[574].

Art. 83 Abs. 5 benennt seinen Adressaten im Gegensatz zu Abs. 4 nicht explizit. Die Normadressaten müssen daher den materiellen Regelungen entnommen werden. Im Ergebnis wird es sich folglich regelmäßig um Verantwortliche oder Auftragsverarbeiter

568 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 72483 von 87533, Rn. 77.
569 *Bäcker et al.,* Datenschutz-Grundverordnung/BDSG, Kapitel VIII. Rechtsbehelfe, Haftung und Sanktionen, S.1032, Rn. 5.
570 Datenschutz Grundverordnung vom 27.04.2016, Siehe Art. 83 Abs. 5 lit. a, DSGVO.
571 Datenschutz Grundverordnung vom 27.04.2016, Siehe Art. 83 Abs. 5 lit. b, DSGVO.
572 Datenschutz Grundverordnung vom 27.04.2016, Siehe Art. 83 Abs. 5 lit. c, DSGVO.
573 Datenschutz Grundverordnung vom 27.04.2016, Siehe Art. 83 Abs. 5 lit. d, DSGVO.
574 Datenschutz Grundverordnung vom 27.04.2016, Siehe Art. 83 Abs. 5 lit. e, DSGVO.

handeln. Zu beachten ist allerdings in diesem Zusammenhang Abs. 5 lit. d, der Sanktionen vorsieht, wenn gegen die Rechtsvorschriften verstoßen wird, die die Mitgliedstaaten im Rahmen des Kapitels IX (Vorschriften für besondere Verarbeitungssituationen, DS-GVO) erlassen. Denn in diesen Fällen **kann** der **Mitgliedsstaat** festlegen, wer zu belangen ist.[575] [576]

Auch Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden, sind nach lit. d Anknüpfungsregelungen für Bußgeldtatbestände. Ein Verstoß gegen die Pflichten dieser Regelungen eröffnet den größeren Rahmen für Geldbußen nach Abs. 5. Beispielsweise ist in diesem Regelungsbereich an die im mitgliedstaatlichen Recht geschaffenen Regelungen für die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses (Art. 88). Dem Verantwortlichen werden wie auch bei der Verarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken (Art. 85) spezifische Pflichten auferlegt, aus denen beim Verstoß gegen das entsprechende nationale Recht ein Bußgeld auf Grundlage einer EU-Verordnung resultiert.[577]

Abs. 5 droht für Verstöße gegen die dort genannten Vorschriften Geldbußen an, ohne dies auf die Pflichten bestimmter Personen zu beschränken. **Die Sanktionsdrohung folgt mithin vollständig der Pflicht im Sachrecht**. Zu beachten ist insb., dass als handelnde Person selbst zum Verantwortlichen wird, wer über die Zwecke und Mittel der Verarbeitung bestimmt, insbesondere weisungswidrig personenbezogene Daten für sich selbst verarbeitet.[578]

Die Bußgeldtatbestände in Art. 83 Abs. 5 DS-GVO sanktionieren Verstöße gegen materielle Grundsätze, Betroffenenrechte und Bestimmungen über Drittstaatentransfer mit bis zu 20.000.000 EUR bzw. bei Unternehmen mit bis zu 4% des weltweit erzielten Jahresumsatzes.[579]

---

575 *J. Philipp Albrecht,* Datenschutzrecht, Allgemeine Bedingungen für die Verhängung von Geldbußen, Art. 83 Abs. 5 DSGVO, S.1221 Rn. 47 d.

576 Recht auf Datenverarbeitung, S. 16, Nr. 3. Art. 83 Abs. 6 DS-GVO.

577 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Tatbestände des Abs. 5 und Abs. 6, Position 72522 von 87533, Rn. 82.

578 *Bäcker,* Datenschutz-Grundverordnung, Rechtsbehelfe, Haftung und Sanktionen, S.1032 Rn. 22.

579 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Allgemeine Bedingungen für die Verhängung von Geldbußen, S. 1266 Rn. 99.

a.) Abs. 5 lit. a

Art. 83 Abs. 5 lit. a DS-GVO referenziert auf die folgenden Artikel der DS-GVO:

- Art. 5: Grundsätze für die Verarbeitung personenbezogener Daten,
- Art. 6: Rechtmäßigkeit der Verarbeitung,
- Art. 7: Bedingungen für die Einwilligung,
- Art.9: Verarbeitung besonderer Kategorien personenbezogener Daten.580

b.) Abs. 5 lit. b

- Art. 83 Abs. 5 lit. b DS-GVO referenziert auf die Rechte der Betroffenen nach Kapitel 3 der DS-GVO.[581]

c.) Abs. 5 lit. c

- Art. 83 Abs. 5 lit. c DS-GVO verweist auf die Regelungen zur Übermittlung personenbezogener Daten in einem Drittstaat gemäß den Art. 44 bis 49 DS-GVO.[582]

d.) Abs. 5 lit. d

- Nach Art. 83 Abs. 5 lit. d DS-GVO ist auch die Verletzung der Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX (Art. 85 - 91 DS-GVO) der DS-GVO erlassen wurden, mit einem Bußgeld bedroht. Darunter fallen insbesondere Vorschriften zur Verarbeitung von Beschäftigungsdaten nach Art. 88 DS-GVO, was in Deutschland in § 26 BDSG geregelt wurde.[583]

e.) Abs. 5 lit. e

- Aufsichtsbehörden können gemäß Art. 83 Abs. 5 lit. e DS-GVO auch dann ein Bußgeld verhängen, wenn Verantwortliche oder Auftragsverarbeiter eine Anweisung oder eine vorübergehende oder endgültige Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Art. 58

580 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Allgemeine Bedingungen für die Verhängung von Geldbußen, S.1266 Rn. 100.
581 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Allgemeine Bedingungen für die Verhängung von Geldbußen, S.1266 Rn. 101.
582 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Allgemeine Bedingungen für die Verhängung von Geldbußen, S.1266 Rn. 102.
583 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Allgemeine Bedingungen für die Verhängung von Geldbußen, S.1266 Rn. 103.

Abs. 2 DS-GVO nicht befolgen oder sie in den Untersuchungsbefugnissen gemäß Art. 58 Abs. 1 DS-GVO beschränken.[584]

4.5.10 Nichtbefolgung nach Art. 83 Abs. 6 DS-GVO

Zu guter Letzt können nach Art. 83 Abs. 6 DS-GVO bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde nach Art. 58 Abs. 2 DS-GVO Bußgelder in Höhe von bis zu 20 Mio. Euro festgesetzt werden. Um das finanzielle Risiko der Nichtbefolgung einer solchen Anweisung zu rechtfertigen, müssen die Aufsichtsbehörden auf eine möglichst präzise, eindeutige und verständliche Formulierung der Anweisung achten.[585]

Art. 83 Abs. 6 DS-GVO ist eine sogenannte Blankett-Vorschrift. Die Vorschrift bezieht sich auf eine von der Aufsichtsbehörde erlassene Maßnahme, einen Verwaltungsakt. Für die Sanktionierung bedeutet das, dass der Verwaltungsakt für den Adressaten zur Tatzeit verbindlich ist. Der Verwaltungsakt muss also entweder nach Ablauf der einmonatigen Widerspruchsfrist (§ 70 VwGO[586]) bzw. nach Ablauf der Klagefrist (§ 74 Abs. 1 VwGO) bestandskräftig geworden sein oder, wenn kein Widerspruchverfahren vorgesehen ist, von Gesetzes wegen sofort (§ 80 Abs. 1 Satz 1 Nr. 3 VwGO) bzw. aufgrund der Anordnung der sofortigen Vollziehung durch die Behörde im Einzelfall (§ 80 Abs. 2 Satz 1 Nr. 4 VwGO) vollziehbar sein. Die Zuwiderhandlung gegen ein durch den Verwaltungsakt angeordnetes Tun, Dulden oder Unterlassen ist daher grundsätzlich nicht schon mit Erlass der behördlichen Entscheidung bußgeldbewehrt, sondern erst dann, wenn der Verwaltungsakt für den Betroffene verbindlich ist. Die Ahndung eines Ungehorsams setzt voraus, dass der Betroffene den Vollzug der gegen ihn gerichteten Verfügungen ohne die Möglichkeit hemmender Rechtsbehelfe zunächst einmal hinnehmen muss. Soweit die Behörde den Adressaten zur Mitwirkung auffordert, reicht es nicht aus, die fristgemäße Erfüllung von Mitwirkungspflichten durch dienstliches **Schreiben** ohne Zustellung, Begründung und Rechtsbehelfsbelehrung anzudrohen.

---

584 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, Allgemeine Bedingungen für die Verhängung von Geldbußen, S.1266 Rn. 104.

585 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, Nemitz, S. 1089, Rn. 37, Art. 83 Abs. 6 DS-GVO.

586 Verwaltungsgerichtsordnung.

Nach § 1 OWiG ist der Hinweis, dass der Mitwirkungspflichtige eine Ordnungswidrigkeit begehe, wenn er dieses Schreiben nicht beantwortet, nicht richtig.[587] Damit sanktioniert die DS-GVO sowohl in Art. 83 Abs. 5 lit. e als auch Art. 83 Abs. 6 DS-GVO Verstöße gegen Maßnahmen aus Abhilfebefugnissen gemäß Art. 58 Abs. 2 DS-GVO.[588]

587 *Haniel/Geiger/Schmutterer,* Gesetz über Ordnungswidrigkeiten, 1983, § 1 OWiG.
588 Recht auf Datenverarbeitung, Bußgeld im digitalen Zeitalter, S. 16, Nr. 3.

Teil. 2 - Umsetzung

1 Die Umsetzung:

Die „Bitcom Research GmbH“ veröffentlichte im September 2019 eine Studie über den Erfolg bei der Umsetzung der Datenschutz-Grundverordnung. Demnach kämpft die deutsche Wirtschaft immer noch mit der Umsetzung der Datenschutz-Grundverordnung. Fast eineinhalb Jahre nach Geltungsbeginn haben zwar zwei Drittel der Unternehmen (67 %) die neuen Datenschutzregeln **mindestens zu großen Teilen umgesetzt**. Dabei hat allerdings **erst ein Viertel** (25 %) die Umsetzung der DS-GVO **vollständig abgeschlossen**. Das ist das Ergebnis einer repräsentativen Befragung unter mehr als 500 Unternehmen aus Deutschland, die der Digitalverband Bitkom im Rahmen seiner Privacy Conference vorgestellt hat. Weitere 24 Prozent haben die Verordnung teilweise umgesetzt, 6 % stehen noch am Anfang. Rechtsunsicherheit und ein schwer abzuschätzender Umsetzungsaufwand sind für jeweils zwei Drittel der Unternehmen (68 %) die größten Herausforderungen. Mehr als die Hälfte (53 %) beklagen fehlende Umsetzungshilfen, gut ein Drittel (37 %) sieht fehlendes Fachpersonal als größte Herausforderung. Über 97% sehen den größten Aufwand in der Umsetzung der aufwendigen Dokumentation. Die Katalogisierung der Prozesse ist für 93 % sehr aufwändig, 86 % geben dies für ihr Vertragsmanagement an. Die sogenannten **Privacy-by-Design**-Anforderungen zu erfüllen, bedeutet für 84 % viel Arbeit. Ähnlich viele (82 %) kämpfen wegen der Datenschutz-Grundverordnung mit hohen Aufwänden für den Betrieb ihrer Webseiten. Nicht nur der Aufwand ist hoch. Für viele haben die Datenschutzregeln auch enge Grenzen für Innovationen gesetzt. Jedes siebte Unternehmen (14 %) erklärt: In unserem Unternehmen sind neue, innovative Projekte aufgrund der Datenschutz-Grundverordnung gescheitert.[589]

Der zweite Teil beschäftigt sich aus diesem Grund mit der Einführung bzw. Umsetzung, den organisatorischen Themen sowie den erforderlichen Auflagen. Hierbei geht es um die tatsächliche Implementierung der Datenschutz-Grundverordnung. Dabei wird unter

589 *Bitcom Research GmbH*, Zwei Drittel der Unternehmen haben DS-GVO größtenteils umgesetzt, Berlin 17.09.2019, https://www.bitkom-research.de/de/pressemitteilung/zwei-drittel-der-unternehmen-haben-ds-gvo-groesstenteils-umgesetzt.

anderem die Frage zu beantworten sein: „ist eine praktische Umsetzung mit den gegebenen Mitteln möglich und sind Schwachstellen in der Datenschutz-Grundverordnung erkennbar?“. Des Weiteren müssen einzelne Unternehmensbereiche an die geänderten Umstände angepasst werden, was ebenfalls durch eine Betrachtung im Abschnitt, Change-Management, dargelegt wird.

Je nach Unternehmensgröße ist ein externer oder interner Datenschutzbeauftragter zu benennen oder zu beauftragen. Die neue Datenschutz-Grundverordnung hat auch hierzu Änderungen generiert, die eine Entscheidung bezüglich interner und oder externer Wahl nicht eben einfacher gestalten. Da sich das Aufgabengebiet sowie die Haftung erheblich geändert haben, müssen diese Punkte detailliert betrachtet werden. Bei dem in der Folge beschriebenen Unternehmen handelt es sich um eine Ländergesellschaft, welches an einen internationalen Konzern angeschlossen ist. Dieser Umstand erfordert es, dass die konzernübergreifenden Datenübertragungen ebenfalls zu betrachten sind, wie auch die eigentliche Struktur eines Konzernes und den damit verbundenen Auflagen.

1.1 Anforderung an die Datenschutzorganisation

Die DS-GVO[590] führt Rechtsbehelfe, Haftungserweiterungen und erhöhte Bußgelder ein. Deshalb sollten Unternehmen besonders gewissenhaft bei der Anpassung ihrer Datenschutzmaßnahmen vorgehen, um den erhöhten Schutzstandards gerecht zu werden. Viele Unternehmen werden erhebliche Anstrengungen unternehmen müssen, um ein Datenschutz-Managementsystem zu implementieren, welches den Anforderungen der DS-GVO entspricht. Jedoch wird die EU-weite Harmonisierung der Datenschutzregeln die unternehmensinterne Datenschutzorganisation zukünftig auch erleichtern.[591]

Die DS-GVO verfolgt einen risikobasierten Ansatz in Bezug auf das zu garantierende Datenschutzniveau. Die nachfolgenden Abschnitte enthalten Einzelheiten zu den

590 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), DSGVO - Datenschutz Grundverordnung.

591 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, Anforderungen an die Datenschutzorganisation, S. 39.

verschiedenen organisatorischen Anforderungen nach der DS-GVO für Verantwortliche und – in eingeschränktem Maße – auch für Auftragsverarbeiter.[592]

1.2 Das Unternehmen

Das Jahr 2018 brachte die von langer Hand vorbereitete und angekündigte Einführung der Datenschutz-Grundverordnung (DS-GVO) und somit endlich ein in der ganzen Europäischen Union einheitliches Datenschutzniveau. So groß die Freude in Erwartung dieses neuen Regelungswerks auch war, mindestens genau so groß war die Spannung auf die zu erwartenden Schwierigkeiten in der Umsetzung dieser so intensiv diskutierten Verordnung. Gerade die Frage der Umsetzung trieb die Praktiker um, denn bereits zur Einführung waren so manche Regelungen zu erkennen, bei denen sich doch wesentliche Fragen ergaben: Wie denn bspw. die praktische Umsetzung gelingen sollte, ob diese nicht die verantwortliche Stelle vor unlösbare Probleme stellen würde, inwieweit die Neuregelung überhaupt Sinn macht … und …und ….und… So fanden sich zahlreiche Diskussionen, die sich mit der praktischen Umsetzung der Regelungen beschäftigten:

Das in der Folge beschriebene Unternehmen betrieb und bewirtschaftete 4600 Parkhäuser und Tiefgaragen in über 500 Städten auf vier Kontinenten. Diese Tätigkeit wurde von damals 18.000 Mitarbeiterinnen und Mitarbeitern durchgeführt (Die Unternehmensbezogenen Daten waren tagesaktuelle Daten, da tatsächlich täglich mehrere neue Mitarbeiter bzw. Objekte angestellt und oder in Betrieb genommen wurden, Stand 05/2018). Alle Länder arbeiteten sowohl in einem internationalen Netzwerk als auch in nationalen Netzen zusammen. Ländergesellschaften tauschten Daten mit der Konzernmutter aus sowie untereinander, sofern Bedarf bestand. Alle Länder mussten darüber hinaus in der Lage sein, autark und unabhängig agieren zu können.

Darüber hinaus war es im Vorfeld des Verkaufs nicht erwünscht das geplante Change-Management bzw. die Organisationsveränderungen umzusetzen, da dieses doch mit nicht unerheblichen Kosten verbunden war. Ein Unternehmen soll in der Regel „hübsch“ gemacht werden, bevor es in den Verkauf gelangt.

592 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, Anforderungen an die Datenschutzorganisation, S. 39.

Gewünschte Eigenschaften sind unter Anderem aber nicht abschließend:

- Substanzwert des Unternehmens
- Ertragswert
    - Darstellbarer stetig wachsender Umsatz über die vergangenen fünf Jahre
    - Gleiches gilt für den EBITDA[593]
    - Möglichkeiten der Umsatzsteigerung durch Verbesserung der einzusetzenden Mittel
    - Zugewinn von Marktanteilen
    - Verlängerte Verträge (Pachtverträge und Management Verträge), lange Laufzeiten
- Zugang zu einem bisher nicht erschlossenen Markt
- Personalkosten
- Übernahme von Know How
- Schlankes und effizientes Management

Es handelt sich bei den angeführten Punkten lediglich um Erfahrungswerte. Natürlich ist der Kauf eines Unternehmens mit erheblich größerem und komplexerem Aufwand verbunden.

Teile der Einführung müssen aus dem Gedächtnis zitiert werden, verbunden mit den Erfahrungen der Einführung aus befreundeten Unternehmen. Leider ist es nicht immer möglich Namen und Fakten zu nennen, da hierfür schlicht die Erlaubnis nicht erteilt wurde, insbesondere wenn über das Thema des Datenschutzes geschrieben wird.

593 *Gabler Wirtschaftslexikon*, EBITDA - Earnings before Interest, Taxes, Depreciation and Amortization, Unternehmensbewertung, https://wirtschaftslexikon.gabler.de/definition/earnings-interest-taxes-depreciation-and-amortization-ebitda-35471/version-327317 (zugegriffen am 30.8.2020).

1.3 Konzernstrukturen

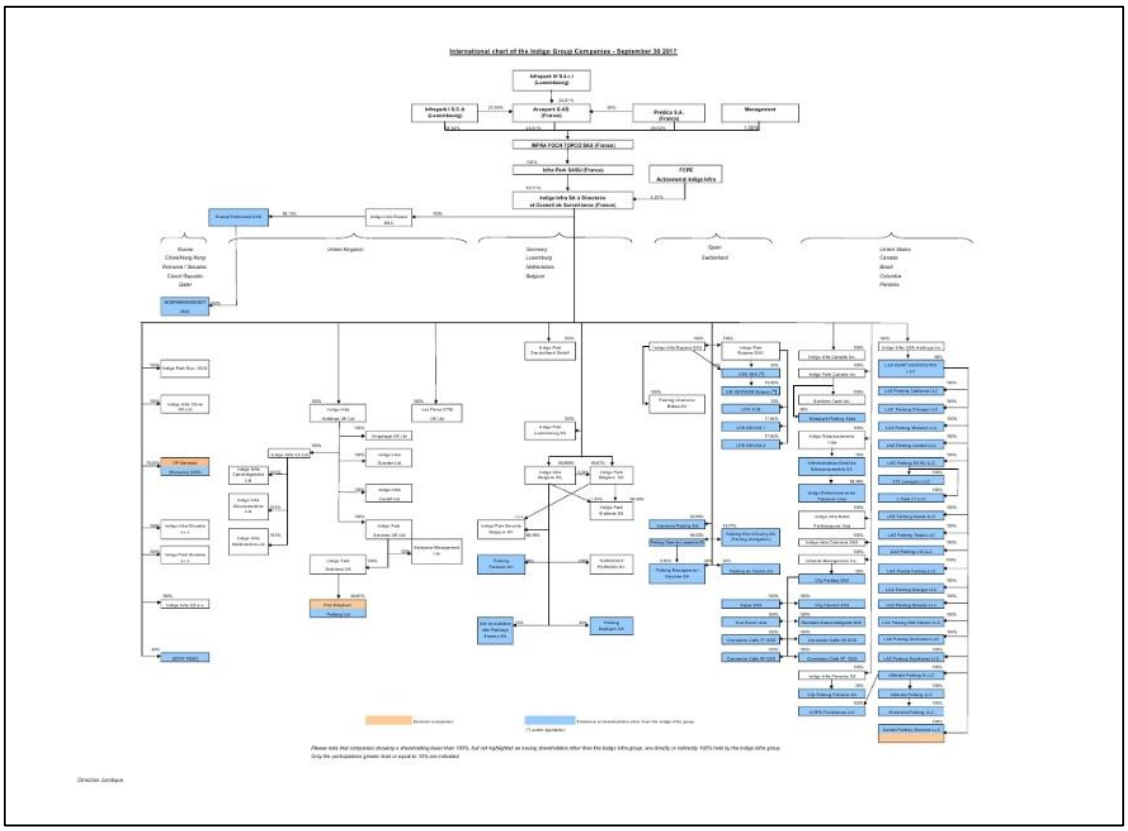

Abbildung 2: Quelle: Indigo Park Group (Stand 2017)

Das in der Folge beschriebene Unternehmen bewirtschaftete in Deutschland im Jahr 2018, 35 Parkhäuser in 15 Städten. Das Kerngeschäft war die Bewirtschaftung von Fahrzeugabstellplätzen, welche für die Kurzzeit Parker (in der Regel maximal 24 Stunden) als auch für den Dauerparker (i.d.R. größer 24 Stunden) bereitgestellt wurden.[594]

Das nachfolgende Organigramm soll eine stark vereinfachte Struktur des Standorts Deutschland darstellen. Namen und Daten sind aus Datenschutzgründen nicht eingefügt, können aber auf Nachfrage im Einzelnen dargelegt werden.

594 *Pech et al.,* Parkhäuser - Garagen, 2009, 21 Begriffe 2|3|1

1.4 Organigramm

Abbildung 3: Organigramm Unternehmen (sehr stark vereinfacht)

Das beschriebene Unternehmen wurde, nicht abschließend, mit den nachfolgenden Abteilungen betrieben. Der Konzerndatenschutz wird für die vorliegende Arbeit theoretisch, nicht aber vollumfänglich oder nur in den betroffenen Bereichen dargestellt. (siehe Datenschutzmanagement in Konzernstrukturen)

- Geschäftsführung / Geschäftsleitung
- Operativer Bereich
- HR (Human Resources)
- Technische Abteilung
- Buchhaltung / Controlling
- Marketing
- Assistenz / Sekretariat
- Neugeschäft (New Business)

Das Kerngeschäft eines Parkhausbetreibers liegt in der Bewirtschaftung von Stellplätzen sowie in der Akquise neuer Objekte. Dabei handelt es sich um sogenannte ON-Street sowie Off-Street Modelle. Als On-Street werden Parkplätze entlang der Verkehrsstraßen bezeichnet. Als Off-Street werden Parkhäuser, Parkplätze und Tiefgaragen bezeichnet, die abseits verkehrsführender Straßen zu finden sind.

Nachfolgende Abbildung zeigt die geografische Lage der Parkhäuser in einer stark vereinfachten Deutschlandkarte auf. Diese erklärt deutlich die fragmentierte Lage der im

Organigramm aufgeführten Regionen. Die farbliche Agenda zeigt die Vertragsarten auf, mit welchen die Objekte vertraglich abgeschlossen wurden.

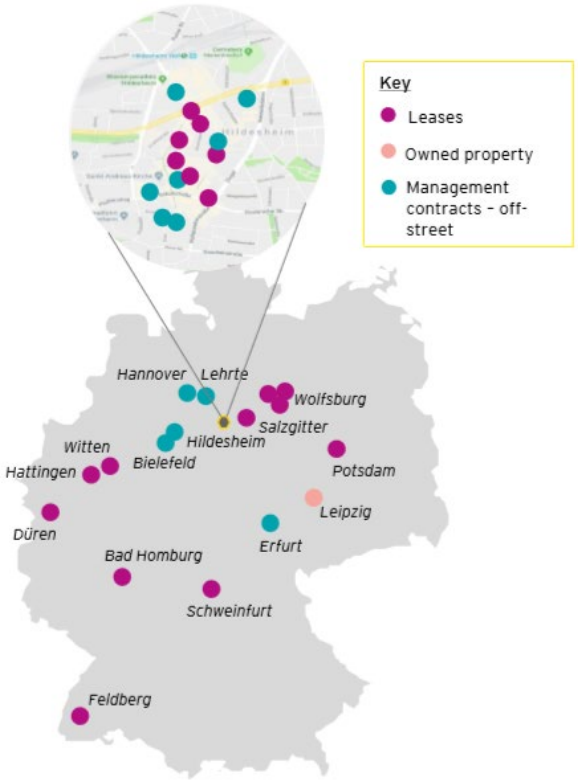

Abbildung 4: **Mögliche** geografische Lage bewirtschafteter Parkobjekte.

Lease Contract: Als „lease Contract“ sind die Verträge aufgeführt, die in Form eines Pachtvertrages (siehe § 581 ff. BGB) abgeschlossen wurden. Die durchschnittliche Vertragsdauer bei Pachtverträgen liegt erfahrungsgemäß bei 10 Jahren. Meist werden zusätzliche Optionen in den Vertrag übernommen, die dem Pächter oder Verpächter eine einseitige Optionsziehung ermöglicht. Diese Optionen werden ebenfalls in der Regel auf 5 Jahre vereinbart.

Die Pachtzahlungen können als Festpacht vereinbart sein oder in Form einer Umsatzpacht, wie auch als Mischform aus Festpacht und Umsatzpacht. Der Nachteil der Pachtverträge liegt in der wirtschaftlichen Abhängigkeit des Pächters. Dieser muss unabhängig der wirtschaftlichen Lage, die regelmäßigen Pachtzahlungen leisten. In manchen Fällen kann dieses bei langen Laufleistungen und sich verändernden Bedingungen zu erheblichen wirtschaftlichen Schwierigkeiten für den Pächter führen.

Owned Property: Hiermit wird das Eigentum an dem entsprechenden Objekt bezeichnet.

Management Contract: Management Verträge erinnern sehr stark an Hausmeisterdienste. Diese Art des Vertrages ermöglicht eine detaillierte Auflistung der durchzuführenden Arbeiten. Dieses wird zu einem festvereinbarten monatlichen Beitrag bewirtschaftet mit einer festen Laufzeit, die meist auf 2 - 5 Jahre vereinbart wird. Der Vorteil eines Management Vertrages liegt in der Unabhängigkeit des Vertrages vom wirtschaftlichen Erfolg. Hier müssen der Eigentümer bzw. der Vertragspartner das vereinbarte monatliche Entgelt leisten, egal was passiert.

Durch die teils sehr fragmentierte Lage der Objekte, muss in der Regel (in Abhängigkeit der Unternehmenskultur und Struktur) ortsansässiges Personal eingesetzt werden, die den Abstand von den entsprechenden Objekten zur Abteilungsleitung und den Nutzern reduzieren. Hierfür werden in der Regel sogenannte Regionalleiter- Direktoren eingesetzt, die für eine geografische Region, einer gewissen Anzahl an Objekten sowie dem dazu gehörigen Personal verantwortlich sind.

1.4.1 Tiefgarage(n)

Als Tiefgarage werden Objekte bezeichnet, welche einen unterirdischen Baukörper besitzen.[595]

1.4.2 Parkhäuser

Unter Parkhäusern werden meist diejenigen Objekte bezeichnet, die als Hochgarage konzipiert und erbaut wurden.[596]

595 *Pech et al.,* Parkhäuser - Garagen, 2009, S.45, Vorplanung / Entwurf --Tiefgaragen.
596 *Pech et al.,* Parkhäuser - Garagen, 2009, S.45, Vorplanung / Entwurf -- Parkhäuser.

1.5 Datenschutzmanagement in Konzernstrukturen

1.5.1 Definition des Konzerns

Das Gesellschaftsrecht geht von einer unabhängigen Gesellschaft als Regelfall aus, §§ 15 ff., 291 ff. AktG sprechen von „verbundenen Unternehmen". Bei der Definition hilft § 18 AktG,[597] wonach ein Konzern ein Zusammenschluss mehrerer rechtlich selbstständiger Unternehmen zu einer Wirtschaftseinheit mit einheitlicher Leitung verstanden wird.[598]

Für die Erfüllung des Tatbestandsmerkmals der „einheitlichen Leitung" genügt nach dem weiten Konzernbegriff die Ausübung in zentralen Bereichen der unternehmerischen Tätigkeit (insb. Einkauf, Personalwesen, Organisation, Verkauf) – die Abgrenzung zum engen Konzernbegriff ist indes nicht von hoher Relevanz, da § 18 Abs. 1 S. 1 und 3 AktG weitreichende Vermutungen vorsieht. Durch den Konzernbegriff werden sowohl der Unterordnungs- (Absatz 1) als auch der Gleichordnungskonzern (Absatz 2) erfasst.[599]

Der Begriff des Konzerns wird in der DS-GVO nicht verwendet. Geregelt bzw. behandelt werden „Unternehmen" und „Unternehmensgruppe" mit einer Definition der Unternehmensgruppen die in Art. 3 Nr. 18 und 19 DS-GVO[600] zu finden sind. In **Erwägungsgrund 48** DS-GVO, der für die Integration herangezogen wird, ist unsystematisch von „Stelle", Unternehmensgruppe oder einer Gruppe von Einrichtungen, die einer zentralen Stelle zugeordnet sind, die Rede.[601]

---

597 Aktiengesetz, § 18 AktG.

598 *Lachenmann,* Datenübermittlung im Konzern, 2016, Normative Grundlagen der Datenverarbeitung in Konzernen, S. 70 Abs. 1.

599 *Lachenmann,* Datenübermittlung im Konzern, 2016, Normative Grundlagen der Datenverarbeitung in Konzernen, S. 70 Abs. 2.

600 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 3 Nr. 18 und 19 DSGVO.

601 *Forgó/Helfrich/Schneider* (Hrsg.), Betrieblicher Datenschutz, Konzerndatenschutz, S. 577, Rn. 3.

Erwägungsgrund 48

Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt.[602]

1.5.2 Grundsätzliche Ziele

Eine wesentliche **Aufgabe** der **Unternehmensführung** ist es, stets dafür Sorge zu tragen, dass rechtliche **Vorgaben** eingehalten werden. Dies gilt auch für den Bereich des Datenschutzes im Konzernkontext. Für die jeweilige **Leitung** jedes Einzelunternehmens ist es daher **notwendig**, bestehende **Datenschutzrisiken transparent** berichtet zu bekommen, um erforderlichenfalls **gegensteuern** zu können.[603]

Um diese Vorgaben (gesetzeskonformes Handeln, transparentes Risikomanagement) nachhaltig, effizient und ressourcensparend zu erreichen, ist es unabdingbar ein entsprechendes Datenschutzmanagement aufzusetzen.[604]

Vor diesem Hintergrund ergeben sich folgende drei Hauptziele für das Datenschutzmanagement in Konzernstrukturen:

1. Erfüllung rechtlicher Vorgaben

- Eine der obersten Ziele des Unternehmens ist die **Rechtskonformität**.[605] Demnach ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten grundsätzlich nur zulässig, wenn entweder eine Einwilligung der betroffenen Person oder aber eine entsprechende Erlaubnisnorm vorliegt. [606]

602 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 48 DSGVO.
603 *Bussche/Egle* (Hrsg.), Konzerndatenschutz, S. 44, Rn. 27.
604 *Bussche/Egle* (Hrsg.), Konzerndatenschutz, S. 44, Rn. 28.
605 *Bussche/Egle* (Hrsg.), Konzerndatenschutz, S. 44, Rn. 29, Satz 1.
606 *Piltz,* BDSG, 2018, § 4 Abs. 1 BDSG, Art. 5 DSGVO.

2. Transparentes Risikomanagement durch Integration des Datenschutzes in das interne Kontrollsystem.

- Der Datenschutz im Konzern ist vielfach geprägt von einem Spannungsverhältnis zwischen der Erfüllung gesetzlicher **Vorgaben** und einem Mangel an **Ressourcen** zu deren Umsetzung. Daraus erwächst die Notwendigkeit zur **Priorisierung** von Aufgaben, was wiederum ein **zuverlässiges Risikomanagement** als Entscheidungsgrundlage erfordert.[607]
- Risiken im Bereich des Datenschutzes sind dabei insbesondere negative **Außen- und Innenwirkung**, Informationspflichten bei unrechtmäßiger Kenntniserlangung,[608] [609] Bußgelder und Strafen,[610] Anordnungen und Untersagungen der Aufsichtsbehörden[611] und Schadenersatzforderungen.[612]
- Daneben treffen die Leitung der verantwortlichen Stelle verschiedene gesetzliche **Vorschriften** zur **Erfassung von Risiken** (§ 43 Abs. 1 GmbH, § 91 Abs. 2 AktG).[613] [614] Aufgrund dieser **Ausgangslage** ist die Integration des Datenschutzmanagements in das konzerninterne Kontrollsystem nahezu **unerlässlich**, da nur so der Leitung der jeweils verantwortlichen Stelle die **Möglichkeit** eröffnet werden kann, sich den **vorhandenen Risiken** und der damit verbunden **Verantwortung** zu stellen und die **bestehenden Risiken** angemessen zu **behandeln**.[615]

3. Konzernübergreifendes und effizientes Datenschutzmanagement

- Ein wesentlicher Vorteil eines einzelgesellschaftsübergreifenden Datenschutzmanagements im Konzern liegt in der **Vereinheitlichung von Prozessen** und Strukturen. Dies ermöglicht eine **effiziente** und **kostenoptimierte Datenschutzorganisation**. Durch einen kontinuierlichen Managementprozess werden die Datenschutzaktivitäten, die Effizienz und Qualität der ergriffenen

---

607 *Bussche/Egle* (Hrsg.), Konzerndatenschutz, S. 44, Rn. 31.
608 *Bussche/Egle* (Hrsg.), Konzerndatenschutz, S. 44, Rn. 32.
609 Bundesdatenschutzgesetz, § 42a BDSG, siehe auch Art. 4 Nr. 12 DSGVO, Art. 33, Art. 34 DSGVO.
610 Bundesdatenschutzgesetz, §§ 43, 44 BDSG, siehe auch Art. 83 DSGVO, Erwägungsgrund 148 ff.
611 Bundesdatenschutzgesetz, § 38 Abs. 5 BDSG, siehe auch Art. 51 - 59, Art. 31 DSGVO.
612 Bundesdatenschutzgesetz, § 7 BDSG, siehe auch Art. 82 DSGVO, Erwägungsgrund 146.
613 Gesetz betreffend die Gesellschaften mit beschränkter Haftung, § 43 Abs. 1 GmbH.
614 Gesetz betreffend die Gesellschaften mit beschränkter Haftung, § 91 Abs. 2 AktG.
615 *Bussche/Egle* (Hrsg.), Konzerndatenschutz, S. 45, Rn. 34.

Maßnahmen, sowie die maßgeblichen Überlegungen bei **Abwägungsentscheidungen dokumentiert**. Darüber hinaus wird durch regelmäßige Prüfungen im Rahmen des Managementprozesses die **Angemessenheit** von Schutzmaßnahmen und organisatorischen Vorgaben **sichergestellt**.[616]

1.5.3 Datenverarbeitung im Konzern, Zulässigkeitsnorm

Jede Konzerngesellschaft ist nach dem nunmehr geltenden Recht der DS-GVO selbstständiger „Verantwortlicher" (Art. 4 Nr. 7 DS-GVO) oder Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO).[617] Denkbar ist, dass Konzerngesellschaften die Merkmale der gemeinsamen Verarbeitung nach Art. 26 DS-GVO erfüllen sog. Joint Controllership. Damit ist allerdings keine Erleichterung für die Beteiligten verbunden.[618]

Für einen Konzern kann sich anbieten, statt eine Auftragsverarbeitung nach (Art. 28 DS-GVO) Joint Controllership und ggf. dafür **B**inding **C**orporate **R**ules, (**BCR**), zu schaffen. Grund dafür ist weniger das Problem, ggf. statt Auftragsverarbeitung eine Funktionsübertragung vorzunehmen. Dieses Problem ist wesentlich entschärft, weil die Grenzen der Auftragsverarbeitung nun weiter als bei § 11 BDSG a.F. gezogen sind. Es liegt vielmehr an der Vertragsgestaltung in Verbindung mit der klaren Zuordnung, dass der Auftraggeber über Zwecke und Mittel der Datenverarbeitung entscheidet und die Verarbeitung für diese Zwecke erfolgt, sodass die bislang nach deutschem Recht als Funktionsübertragung eingeordneten Fälle häufig nunmehr unter der DS-GVO als Auftragsverarbeitung i.S.v. Art. 28 DS-GVO qualifiziert werden können.[619]

---

616 *Bussche/Egle* (Hrsg.), Konzerndatenschutz, S. 45, Rn. 35.

617 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 Nr. 8 DSGVO.

618 *Forgó/Helfrich/Schneider* (Hrsg.), Betrieblicher Datenschutz, S. 579, Rn. 12.

619 *Forgó/Helfrich/Schneider* (Hrsg.), Betrieblicher Datenschutz, S. 579, Rn. 13.

1.5.4 Zentrale Personalverwaltung

Der Konzerneigenschaft entspricht es, wenn neben der Personalabteilung auch eine zentrale Personalverwaltung besteht. Wenn die Mitarbeiter-Daten der einzelnen Mitgliedsfirmen diese Zentralstelle zur Verfügung gestellt werden, liegt eine Übermittlung nach BDSG a.F. vor, für die die Rechtsgrundlage § 32 BDSG a.F.[620] sein konnte. Nun regelt auf Basis einer Öffnungsklausel (Art. 88 DS-GVO) § 26 BDSG die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses (§ 26 Abs. 3 BDSG[621] auf Basis von Art. 9 Abs. 2 lit. b DS-GVO[622]).[623]

Das Problem ergibt sich bei zentraler Verwaltung der Personaldaten, die mit mehreren Tochtergesellschaften auszutauschen sind, also zunächst zum Zwecke der Zentralverwaltung an die Muttergesellschaft weitergegeben werden.[624]

1.5.5 Datenschutzmanagementsystem

In Anlehnung an andere Managementsysteme, wie beispielsweise DIN ISO/IEC 27001[625], DIN ISO/IEC 9001[626] oder DIN ISO/IEC 14001[627], empfiehlt es sich , das Datenschutzmanagementsystem in ähnlicher Art und Weise aufzubauen, um einen integrierten Betrieb mit diesen verwandten Managementsystemen zu unterstützen und somit eine effiziente Umsetzung im Konzern zu etablieren. Unterstützend für den Betrieb des Datenschutzmanagementsystems auf Basis der DIN ISO/IEC 27001 ist auch die Heranziehung des Bausteins z.B. Datenschutz aus den Grundschutzkatalogen des BSI

620 *Körffer et al.,* Bundesdatenschutzgesetz, 10. Aufl. 2010, § 32 BDSG a.F.
621 *Piltz,* BDSG, 2018, § 26 Abs. 3 BDSG.
622 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 9 Abs. 2 lit. b DSGVO.
623 *Forgó/Helfrich/Schneider* (Hrsg.), Betrieblicher Datenschutz, S. 591, Rn. 61.
624 *Forgó/Helfrich/Schneider* (Hrsg.), Betrieblicher Datenschutz, S. 592, Rn. 66.
625 Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen, 06.2017.
626 DIN EN ISO 9001:2008-12 (Deutsche Industrie Norm, Europa Norm, International Organization for Standardization), 12.2008.
627 Umweltmanagementsysteme - Anforderungen mit Anleitung zur Anwendung (ISO 14001:2015).

empfehlenswert,[628] jedoch im Einzelfall um konzernspezifische bzw. auch globale Anforderungen erweitert werden muss.[629]

1.5.6 Datenschutzorganisation

Der Aufbau und Betrieb eines effizienten und wirkungsvollen Datenschutzmanagementsystems im Konzernumfeld ist eine rechtliche und organisatorische Herausforderung. Um dieser Herausforderung gerecht zu werden, ist eine entsprechende Organisationsstruktur notwendig. Dabei nimmt der Konzerndatenschutzbeauftragte eine zentrale Rolle im Datenschutzmanagementsystem ein. Die Datenschutzorganisation selbst erstreckt sich aber auf verschiedene **Funktionsträger des Konzerns**. Dabei kann es je nach Konzernstruktur Abweichungen in der personellen Zusammensetzung der Datenschutzorganisation geben. Die folgenden Rollen sind jedoch typischer Weise vorhanden:[630]

- Konzernleitung
- Konzerndatenschutzbeauftragter
- Leitung der Einzelgesellschaft
- Lokaler Datenschutzbeauftragter einer Einzelgesellschaft
- Datenschutzkoordinatoren
- Geschäftsprozessverantwortliche
- Entscheider/Führungskräfte
- Benutzer

628 *Quiring-Kock*, DuD, Datenschutz und Datensicherheit 2012, 832.
629 *Bussche/Egle* (Hrsg.), Konzerndatenschutz, Teil 2. Datenschutzorganisation im Konzern, S. 45+46, Rn. 39.
630 *Bussche/Egle* (Hrsg.), Konzerndatenschutz, Teil 2. Datenschutzmanagement im Konzern, S. 47, Rn. 43.

1.6 Angebotene Dienstleistungen

Je nach geografischer Lage und auch Vertragsform sowie örtlichen Gegebenheiten werden unterschiedliche Dienstleistungen angeboten. In öffentlichen Parkhäusern (für den öffentlichen Verkehr konzipiert) werden sogenannte **Kurzparker**-Tarife (höhere Fahrzeugfrequenz) angeboten. Dabei handelt es sich in der Regel um einen Zeitraum von bis zu 15 Minuten bis mehrere Stunden. Dieses ist sehr stark abhängig von der Nutzung des Objekts. Bspw. wird an einem Flughafen ein deutlich höherer Tarif ausgerufen als an einem weniger frequentierten Ort. Die durchschnittliche Parkdauer bei dem beschriebenen Unternehmen, bezogen auf die bewirtschafteten Objekte, lag im Jahr 2018 bei ca. drei Stunden. Diese Dauer variierte unter anderem in Abhängigkeiten von Wochentagen und der Feriensituationen. Wie an Flughäfen festzustellen, haben Parkhäuser und Parkplätze die nahe an den Terminals stehen, einen höheren Tarif mit geringerer Taktung. Hierdurch soll eine kontinuierlich hohe Umschlagshäufigkeit, bezogen auf den einzelnen Stellplatz, erreicht werden. Parkobjekte, die weiter entfernt angeschlossen sind, sinken dementsprechend im Tarif, als auch in der Taktung. Einige Anbieter von Langzeit-Parkobjekten sind dazu übergegangen die parkende Kundschaft per Shuttle zum gewünschten Objekt zu bringen. Es ist sicherlich angenehm, sein Fahrzeug vor Urlaubsbeginn in der Nähe eines Flughafens zu parken und direkt vor die Türe gefahren zu werden und dazu noch relativ wenig Geld entrichten zu müssen. Bei der Ankunft aus dem Urlaub, steht dasselbe Unternehmen zur Abholung bereit, sofern die Kommunikation im Vorfeld stattgefunden hat.

Das **Dauerparken** ist dann gegeben, wenn zwischen dem Parkhausbetreiber und dem Fahrzeughalter ein Einstellvertrag abgeschlossen wurde. Dieser wird meist monatlich als Pauschalmiete bezahlt, unabhängig davon, wie oft und wie lange innerhalb des verrechneten Zeitraums die Garage benutzt wird.[631] Dauerparken bedeutet nicht automatisch 24/7 (24 Stunden pro Tag und sieben Tage die Woche). Es werden in der Regel Verträge angeboten, die unter verschiedenen Namen publiziert werden wie bspw. „Jobticket, Wochenticket, Wochenendticket“ usw. Hintergrund ist den Vertrag auf die entsprechenden Bedürfnisse der Nutzer auszulegen. Wenn der Stellplatz nur an Wochentagen von bspw. 9:00 Uhr bis 18:00 Uhr benötigt wird, kann dieser Vertrag an

631 *Pech et al.,* Parkhäuser - Garagen, 2009, S21, 2|3|1.

die Wünsche des Kunden angepasst werden, bei gleichzeitiger Reduzierung der monatlichen Aufwendungen. Anderseits gibt es Nutzer, die einen Stellplatz nur an Wochenenden benötigen. Durch derartige Maßnahmen kann ein Stellplatz höher ausgelastet werden.

Darüber hinaus werden Sonderregelungen angeboten wie bspw. **Elektromobilität**, als auch **CarMobility**. Diese besonders ausgestatteten Stellplätze bieten die Möglichkeit an, Fahrzeuge mit **Elektromobilität** an den Ladestationen aufzuladen. Für diesen besonderen Service müssen die Ladestationen mit der neuesten Hard- und Software ausgestattet sein. Nur dadurch kann ein potenzieller Kunde sein Fahrzeug während eines Parkvorgangs aufladen.

Des Weiteren werden aktuell besondere Stellplätze für den Bereich der CarMobility zur Verfügung gestellt. Das „Car-Sharing“ Segment benötigt eine Anlaufstelle, an welcher die Fahrzeuge abgestellt werden können. Dabei handelt es sich meist um einen „Meeting Point“.

Die neue Generation der Fahrzeugabstelleinrichtung wird nicht mehr nur zum Parken genutzt werden. Der Kunde erwartet ein flexibles Konstrukt, das außer Parken weiteren Service anbietet. Nachfolgende Aufzählung ist nur ein grober Überblick, um aufzuzeigen, in welche Richtung sich die Dienstleistung im Segment Parkhäuser und Tiefgaragen bewegt.

- Kurzzeitparken
- Dauerparken
- App / Online basierende Buchungssysteme
- Elektromobilität
- Car-Sharing
- Einzelplatzerfassung
- Übergabe der Navigationsdaten an das Kundenfahrzeug
- Frei / Besetzt Informationen bereits vor der Anfahrt an das jeweilige Objekt
- Barrierefreie Zu- und Abfahrt
- Paketdienst
- Fahrzeug Innen / Außen Reinigung
- Reifenservice

usw.

Alle aufgeführten Punkte sind in irgendeiner Weise auf Vertragsebene mit dem Betreiber bzw. Eigentümer verbunden. Ob die Vertragsdaten des Dauerparkers oder den erforderlichen Kunden / Fahrzeugdaten bei der Nutzung der **Elektromobilität**, die Übermittlung von Daten zwischen der Zentrale in Deutschland, den Parkhäusern und Tiefgaragen an eine Zentrale ist zwingend erforderlich. Nur dadurch ist es möglich eine der oben genannten Dienstleistungen erst anzubieten.

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.[632] Durch die Datensammlung personenbezogener Daten die teilweise erforderlich sind kommen erhebliche Daten zusammen, deren Schutz an oberster Stelle stehen muss. Auch wenn es sich unwahrscheinlich anhören sollte, ist es aktuell möglich anhand der Fahrzeugdaten, welche mit automatischen Scheibenwischersystemen ausgestatten sind, den Einsatz derjenigen in Uhrzeit und Dauer definieren zu können. Verbunden mit der geografischen Lage sind Wohnort und Fahrtroute bestimmbar. Es existieren ausreichend Stimmen, die in der Möglichkeit der Auswertung eine Erfassung der personenbezogenen Daten sehen, auch wenn hierzu einiges an technischen Kenntnissen erforderlich ist.

632 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 9 Abs. 1 DSGVO.

1.7 Verbindungen zwischen den Ländern

Bei dem beschriebenen Unternehmen handelte es sich um ein Unternehmenskonzern, welcher über vier Kontinente verteilt tätig war. Dabei war Europa ebenso ein Teil der Struktur wie auch Süd- und Nordamerika.

Das Wirtschaftslexikon Gabler charakterisiert einen Konzern wie folgt: „Sind ein herrschendes und ein oder mehrere abhängige Unternehmen unter der einheitlichen Leitung des herrschenden Unternehmens zusammengefasst, so bilden sie einen Konzern".[633] Die einzelnen Unternehmen sind Konzernunternehmen. Liegt ein Beherrschungsvertrag oder eine Eingliederung vor, sind die Unternehmen als unter einheitlicher Leistung zusammengefasst anzusehen. Sind rechtlich selbstständige Unternehmen, ohne dass das eine Unternehmen von dem anderen abhängig ist, unter einheitlicher Leitung zusammengefasst, bilden auch sie einen Konzern (§ 18 AktG).[634]

Die Folgen eines Konzernes spiegeln sich in vielerlei Bereichen wider. Es existieren Subunternehmen, welche durch die Zentrale eines Unternehmens / Konzern gesteuert werden.

Die Verbindung zwischen den Ländern wurde durch eine schnelle Internetverbindung gewährleistet. Alle Accounts wurden in der Regel durch den Mutterkonzern auf deren Server Systemen angelegt. Die Mitarbeiter der Ländergesellschaften erhielten anhand ihrer Tätigkeiten und den dazugehörigen Vollmachten, die entsprechenden Rechte zugewiesen. Der Einsatz mobiler Datenträger wie auch ein Parallel-System zur Hauptpartition waren nicht zulässig. Das System wurde dahingehend systematisch überprüft und bei Bedarf gesperrt. Genaueres wird im Abschnitt, **TOM**, **t**echnische und **o**rganisatorische **M**aßnahmen aufgeführt und erläutert werden.

Die regelmäßige Kommunikation wurde per E-Mail, als auch in Videokonferenzen durchgeführt. Mit dieser Maßnahme konnten Vorstellungsgespräche im ersten Schritt durchgeführt werden.

---

633 *Springer Gabler Verlag,* http://wirtschaftslexikon.gabler.de/Definition/konzern.html.
634 *Gabler Wirtschaftslexikon*, https://wirtschaftslexikon.gabler.de/definition/change-management-28354/version-251986.

1.8 Vorbereitende Maßnahmen

Die Datenschutz-Grundverordnung verpflichtet Unternehmen ein einheitliches Datenschutzmanagement System einzuführen. Seit Beginn des Datenschutzes ist die oberste Direktive aller Organisationen der **Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten.**

Es ist völlig bedeutungslos, welche Quellen zur Analyse herangezogen werden. Bevor eine Vorgehensweise und ein Zeitplan erstellt werden können, ist eine Bestandsanalyse der bestehenden Situationen vorzunehmen. Da die Einführung eines Datenschutz - Systems einige tiefe Einblicke in das Unternehmen ermöglicht und auch erfordert, sollten die Mitarbeiterinnen und Mitarbeiter, die mit der Analyse beauftragt werden, mit einer ausreichend umfangreichen Vollmacht ausgestattet werden. Nur dadurch kann eine tiefgreifende Strukturanalyse durchgeführt werden.

Bei Analysen in einem laufenden Unternehmen ist es sinnvoll und wichtig auf Basis der vorliegenden Fakten eine Abfrage-Checkliste zu erstellen, die alle groben Fakten zusammenfügt und sammelt.

Um ein ganzheitliches Datenschutzmanagement aufzubauen, sollte der Gesetzestext mit dem Ist-Zustand in der Organisation verglichen werden. „Aus dem Vergleich ergeben sich Risiken, denen **TOM**s (**t**echnische und **o**rganisatorische **M**aßnahmen) zugeordnet werden, um diese Risiken zu reduzieren.“[635]

Mit Bekanntwerden der Einführung der Datenschutz – Grundverordnung wurde der erste Schritt seitens der Geschäftsführung vorgenommen. Es handelte sich um die Ernennung des Verantwortlichen des für die Verarbeitung Verantwortlichen gemäß Art. 24 DS-GVO.[636]

2 Aufbau eines formellen Datenschutzmanagementsystem

635 Https://www.it-daily.net/it-sicherheit/datenschutz/16901-die-eu-dsgvo-kommt-haben-sie-einen- plan-was-zu-tun-ist

636 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 24 DSGVO.

Ganz generell gilt die Empfehlung, die Einhaltung des Datenschutzes inkl. der Einrichtung des Datenschutzbeauftragten unter dem Gesichtspunkt des Datenschutz-Managements, Befundsicherung, Überwachung und Optimierung zu sehen, also in gewissem Sinne als herausfordernde Aufgabe nicht nur der Einhaltung des Datenschutzes sondern auch und vor allem deren Nachweises. Dazu dient das zu schaffende Datenschutz-Management-System.[637] Für die Einführung eines Datenschutz-managements findet sich in der DS-GVO keine explizite rechtliche Verpflichtung. Allerdings bestehen diverse Vorgaben, deren Erfüllung mit einem Datenschutzmanagement erreicht werden kann.[638]

Die Elemente eines Datenschutz-Managementsystems lassen sich wie folgt darstellen:

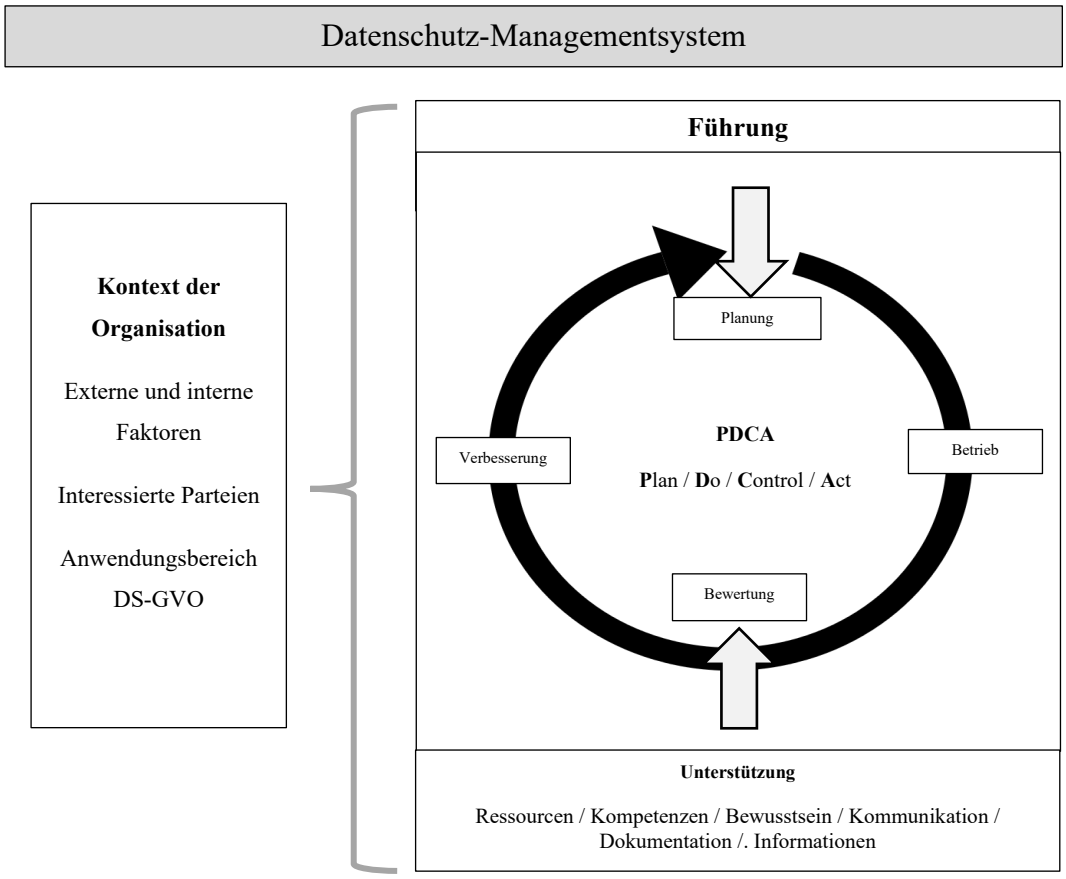

Abbildung 5: Übersicht Datenschutz-Managementsystem

637 *Jung, Alexander*, Datenschutz-(Compliance-)Management-Systeme- Nachweis-und Rechenschaftspflichten nach der DSGVO., Praktische Ansätze für die Erfüllung ordnungsgemäßer Datenverarbeitung, in ZD - Zeitschrift für Datenschutz 2018, 208.

638 *Forgó/Helfrich/Schneider* (Hrsg.), Betrieblicher Datenschutz, Haag, S. 202, Rn. 3.

2.1 Umsetzung / Plan

2.1.1 Erfassen der aktuellen Situation durch die Geschäftsführung / Geschäftsleitung.

Zu Beginn mussten die Verantwortlichkeiten sowie die Zuständigkeiten besprochen und festgelegt werden. Da die deutsche Gesellschaft lediglich durch einen im europäischen Ausland ansässigen Geschäftsführer sowie einem Prokuristen vertreten wurde, welcher in unregelmäßigen Abständen die Zentrale in Berlin besuchte, musste eine ansässige Person, bezogen auf den Standort der Deutschland Zentrale, zum Verantwortlichen gemäß Art. 24 DS-GVO ernannt werden.

Diese Person sollte allerdings nicht zum Datenschutzbeauftragten ernannt werden, da diese Mitglied der Geschäftsleitung war und unter anderem die Einstellung und Freistellung der Mitarbeiterinnen und Mitarbeiter verantwortete. Der Direktor des Unternehmens wurde in Abwesenheit zur verantwortlichen Person ernannt.

Ein Datenschutzbeauftragter muss über die Qualifikation und das Fachwissen zur Wahrnehmung seiner gesetzlich vorgesehenen Aufgaben verfügen. Konkrete Vorgaben hinsichtlich von Kenntnissen oder Ausbildung sind jedoch weder in der DS-GVO noch im BDSG-neu vorgesehen. Datenschutzbeauftragter kann daher grundsätzlich jeder werden.[639]

Unternehmen sollten die Auswahl eines Datenschutzbeauftragten dennoch nicht auf die leichte Schulter nehmen, da dessen Auswahl im Zweifel vor den Datenschutzbehörden gerechtfertigt werden muss. Insoweit ist es hilfreich einen Datenschutzbeauftragten zu benennen, der seine Datenschutzkenntnisse mit einem Zertifikat (z.B. vom TÜV, der IHK o. Ä.) belegen kann und / oder nachweislich über diese Kenntnisse verfügt (z.B. auf Datenschutz spezialisierte Rechtsanwälte).[640]

639 *Die eRecht24 GmbH wird vertreten durch: Rechtsanwalt Sören Siebert, Dipl.-Wirtsch.-Inf. Karsten Fernkorn.*

640 *Die eRecht24 GmbH wird vertreten durch: Rechtsanwalt Sören Siebert, Dipl.-Wirtsch.-Inf. Karsten Fernkorn.*

Zudem ist darauf zu achten, dass die Wahl des Datenschutzbeauftragten nicht zu Interessenkonflikten führt. So sollte z.B. der Geschäftsführer / Unternehmensinhaber eines Unternehmens nicht gleichzeitig Datenschutzbeauftragter sein.[641]

Neben den Verpflichtungen des Datenschutzbeauftragten haben die Verantwortlichen für die Verarbeitung personenbezogener Daten ebenfalls Pflichten:[642]

- Unterstützung des Datenschutzbeauftragten durch Bereitstellung der erforderlichen Ressourcen,
- Unterstützung des Datenschutzbeauftragten durch Ermöglichen des Zugangs zu personenbezogener Daten,
- Unterstützung des Datenschutzbeauftragten durch Ermöglichung des Zugangs zu DV-Systemen,
- Unterstützung des Datenschutzbeauftragten durch Einräumung von Zeit.

Um den Umfang der Datenschutz-Grundverordnung erfassen zu können, war es erforderlich, dass der Verantwortliche des für die Verarbeitung Verantwortlichen, das Thema grundsätzlich und umfassend begreifen müsse.

Dieses konnte, in einem achtstündigen Termin mit der für die Juristische Vertretung zuständigen Rechtsanwaltskanzlei des Unternehmens, lediglich im Grundsatz erörtert werden.

Da dieses für ein derart komplexes Thema nicht ausreichend war, musste zusätzlich entsprechende Fachliteratur angeschafft werden.

Die deutsche Gesellschaft begann bereits im Jahr 2017 mit der Überprüfung und Vorbereitung zur Einführung der Datenschutz-Grundverordnung am 25. Mai 2018. Da dieser Prozess erhebliche Ressourcen binden würde und die Konzernmutter zu dieser Zeit noch keinen zentralen Datenschutzbeauftragten benannt hatte, waren die jeweiligen Ländergesellschaften vorerst auf sich selbst gestellt.

---

641 *Die eRecht24 GmbH wird vertreten durch: Rechtsanwalt Sören Siebert, Dipl.-Wirtsch.-Inf. Karsten Fernkorn*.

642 *Reimann/e.V.,* Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung, 2. Aufl. 2018, Aufgaben des Verantwortlichen oder Auftragverarbeiters, 4.1.1, S. 33 Abs. 1.

Die Problematik der deutschen Gesellschaft ist im Punkt **Organigramm** dieser Arbeit zu erkennen. Die Objekte der deutschen Gesellschaft waren bundesweit fragmentiert aufgestellt. Jedes Objekt wurde zwar mit eigenem Personal vor Ort betrieben, dieses bedeutet allerdings auch, dass die Kollegeninnen und Kollegen umfassend und persönlich informiert werden mussten. Gleiches galt für eine angemessene Schulung.

2.1.2 Vollumfängliche Information aller Mitarbeiterinnen und Mitarbeiter

Zu einem ersten Gespräch wurden alle Abteilungsleiter eingeladen. Dieser Termin wurde im ersten Schritt auf zwei Tage festgelegt. Der Verantwortliche hatte hierzu eine Präsentation, welche auf den Vorbereitungen durch die Fachanwälte der durch das Unternehmen beauftragten Kanzlei aufbaute, in einem ersten Vortrag vorgestellt. Jeder konnte auf Wunsch eine deutsche Ausgabe der Datenschutz-Grundverordnung erhalten. Ebenfalls möglich waren die Einsicht bzw. Aushändigung einer Kopie der Erwägungsgründe, sofern diese gewollt und nachgefragt wurden. Ein Exemplar befand sich im Büro des Verantwortlichen zur freien Nutzung. Die Komplexität des Themas führte zu einer allgemeinen Verunsicherung da die EU-Datenschutz-Grundverordnung zwar auf allgemeines Verständnis stieß, nicht aber der Aufwand, diese im laufenden Betrieb umsetzen zu müssen.

Hintergrund war die Feststellung, dass zum Zeitpunkt der Vorbereitung bzw. Einführung der Datenschutz-Grundverordnung kein zusätzliches Personal eingestellt werden würde. Es war im Vorfeld nicht absehbar ob und wie sich der Aufwand auswirken würde. In der Konsequenz sollten alle Abteilungen die Umstellung bzw. Einführung der Datenschutz-Grundverordnung während des bereits knappen Arbeitstages bewältigen.

Da das Thema auch nach zwei Tagen noch erhebliches Fragepotenzial aufwies, wurde beschlossen, einen regelmäßigen Termin („Jour fix“) zu installieren, um zeitnah alle Probleme erfassen und lösen zu können. Um den Nachweis zu führen, wurde die Teilnahme soweit diese datenschutzkonform war, dokumentiert und in einem Umschlag verschlossen, abgeheftet. Dabei wurde bewusst auf personenbezogene Daten, nach Art. 4

DS-GVO[643] in Verbindung mit Erwägungsgrund 26, soweit dieses möglich war, verzichtet.

Zur besseren Analyse wurde eine erste Selbsteinschätzung geplant, um alle evtl. bestehenden Probleme bzw. Punkte erfassen zu können. Hierzu wurde ein erster Fragebogen entwickelt, welcher alle erforderlichen Punkte erfassen sollte.

2.1.3 Selbsteinschätzung

- **Sachlicher und räumlicher Anwendungsbereich**. Ist die DS-GVO[644] überhaupt anzuwenden bzw. ist diese für die deutsche Gesellschaft relevant? Vgl. Art. 2 sowie Art. 3 DS-GVO[645]
- **Grundsätze für die Verarbeitung personenbezogener Daten** nach Art. 5 DS-GVO:
- Werden die jeweiligen Daten in derart verarbeitet, dass diese für betreffenden Personen vollumfänglich **nachvollziehbar** sind?
- **Einwilligung der Kunden** nach Art. 7 DS-GVO. Muss die Datenverarbeitung auf die geänderten Anforderungen angepasst werden und wie kann so etwas aussehen?
- Art. 15 DS-GVO beschreibt das **Auskunftsrecht.** Wie kann dieses aussehen? Werden Fragen durch die Zentrale beantwortet oder durch die vor Ort angestellten Mitarbeiterinnen und Mitarbeiter? In welchem Zeitraum sind die zuständigen Personen in der Lage auf die Anfragen zu reagieren? Ist die Beantwortung innerhalb 2 Wochen möglich und was muss wie geregelt sein, um dieser Anfrage nachkommen zu können?
- Sind die jeweiligen Personen **berechtigt** bzw. **bevollmächtigt** Daten aus dem System zu löschen? Art. 17 DS-GVO

643 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 4 DSGVO.

644 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).

645 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 2 sowie Art. 3 DSGVO.

- **Recht auf Datenübertragbarkeit** nach Art. 20 DS-GVO:[646] Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturiert gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, die Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogene Daten bereitgestellt wurden, zu übermitteln.[647]
- Welcher Mitarbeiter ist nach Art. 24 DS-GVO der **Verantwortliche** und warum wurde diese Person ernannt?
- Welche **Risiken** bestehen gemäß Art. 24 und 32 DS-GVO? (diese bezogen auf die Rechte und Freiheiten natürlicher Personen).[648]
- Können d**atenschutzfreundliche Einstellungen** nach Art. 25 DS-GVO vorgenommen werden? (**Datenschutz durch Technikgestaltung**).

Erläuterung:

Das Unternehmen hat im Hinblick auf „Datenschutz durch Technikgestaltung" bereits bei der Einführung von Systemen oder der Gestaltung von Prozessen und später im Betrieb geeignete technische und organisatorische Maßnahmen vorzusehen, „[...] die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen" (Art. 25 Abs. 1 DS-GVO).

- Solche Maßnahmen können zum Beispiel darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird und die Daten so schnell wie möglich pseudonymisiert, anonymisiert oder gelöscht werden. Weitere Maßnahmen können die Sperrung von Schnittstellen, die aktive Konfiguration von Sicherheitsmaßnahmen oder organisatorische Maßnahmen der Prozesssteuerung

646 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 20 DSGVO.

647 *Gola u. a.* (Hrsg.), Datenschutz-Grundverordnung, Art. 20 Abs. 1, S. 393 DSGVO.

648 *In Anlehnung an den Fragebogen des Bayerischen Landesamt für Datensicherheit,* In Anlehnung an den Fragebogen des Bayerischen Landesamt für Datenschutzaufsicht, (www.lda.bayern.de), www.lda.bayern.de.

darstellen. Aber auch bei der Auswahl der IT-Komponenten ist der Grundsatz zu beachten. So müssen die ausgewählten Komponenten in der Lage sein, so eingesetzt oder konfiguriert zu werden, dass das Unternehmen sie datenschutzkonform im Sinne der DS-GVO nutzen kann. So ist zum Beispiel systemseitig sicherzustellen, dass Daten im System jederzeit gelöscht werden können, was nicht immer gewährleistet ist.[649]

- Sind für uns tätige Dienstleister und Lieferanten nach Art. 28 DS-GVO[650] in der Lage personenbezogene Daten zu verarbeiten und verfügen diese über geeignete organisatorische Maßnahmen, um die entsprechende Datenverarbeitung rechtskonform durchzuführen?[651]
- Welcher Aufwand ist erforderlich, um ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO erstellen zu können, und was muss darin aufgeführt sein?[652]
- Ist die Sicherheit nach Art. 32 DS-GVO gegeben und inwieweit muss eine **t**echnische und **o**rganisatorische **M**aßnahme (**TOM**) implementiert werden?
- Ist der Nachweis gegenüber der Aufsichtsbehörde ebenfalls möglich? Art. 32 DS-GVO.
- Ist die Verletzung im Umgang mit personenbezogenen Daten feststellbar und wer bzw. wann wird dieses an die Aufsichtsbehörde gemeldet? Art. 33 DS-GVO.
- Ist die Installation einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO erforderlich und wie kann diese aussehen?
- Ist ein interner oder ein externer Datenschutzbeauftragter nach Art. 37 – 39 DS-GVO zu ernennen? Was ist seine Stellung, welche Befugnisse sind erforderlich und was sind seine Aufgaben?
- Macht eine Zertifizierung nach Art. 42 DS-GVO Sinn?

---

649 *Gola et al.,* Datenschutz-Grundverordnung im Überblick, 2. Aufl. 2017, Sichere Prozessgestaltung, S. 61, 5.7.3.

650 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 28 DSGVO.

651 *In Anlehnung an den Fragebogen des Bayerischen Landesamt für Datensicherheit,* In Anlehnung an den Fragebogen des Bayerischen Landesamt für Datenschutzaufsicht, (www.lda.bayern.de), www.lda.bayern.de.

652 *In Anlehnung an den Fragebogen des Bayerischen Landesamt für Datensicherheit,* In Anlehnung an den Fragebogen des Bayerischen Landesamt für Datenschutzaufsicht, (www.lda.bayern.de), www.lda.bayern.de.

- Es müssen allgemeine Grundsätze für die Datenübermittlung erstellt und kommuniziert werden. Art. 44 DS-GVO.
- Wie ist mit Haftungsrisiken umzugehen? Art. 83 DS-GVO.[653]

Die hier erfolgte Selbsteinschätzung würde bei der Umsetzung der Datenschutz-Grundverordnung als hilfreiches Instrument agieren. Diese Fragen bzw. Feststellungen wurden nachfolgend einzeln erörtert und soweit dieses möglich war aus dem Gedächtnis zitiert.

2.1.4 Prozessschritte zur Einführung der DS-GVO im Unternehmen

Nach Auswertung der vorliegenden Daten aus der Selbsteinschätzung konnten die nachfolgenden Prozessschritte generiert werden, unter zu Hilfenahme des Aufsatzes aus der Fachzeitschrift, „Betriebsberater".

- Projektteam für die Umsetzung der DS-GVO[654]
- Festlegung von Projektzielen
- Ressourcenplanung für die einzelnen Projektphasen und Teilschritte
- Budgetplanung
- Risikoanalyse DS-GVO
- Risiken für betroffene Personen
- Mögliche Bußgelder
- Zivilrechtliche Haftungsrisiken
- Rufschäden
- Arbeitsrechtliche Aspekte
- Sonstige Nachteile
- Bestandsaufnahme bereits vorhandener Datenschutzprozesse
- Gap Analyse zwischen Ist- und Soll-Zustand
- Einbindung Datenschutzbeauftragter in sämtliche Projektphasen

653 *In Anlehnung an den Fragebogen des Bayerischen Landesamt für Datensicherheit,* In Anlehnung an den Fragebogen des Bayerischen Landesamt für Datenschutzaufsicht, (www.lda.bayern.de), www.lda.bayern.de

654 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).

- Datenschutzkommunikation im Unternehmen bzw. Konzern
- Datenschutztrainings
- Frühzeitige Kommunikation mit dem Betriebsrat
- Prüfung und Neuverhandlung von Betriebsvereinbarungen[655]
- Einrichtung einer Datenschutzberatung im Unternehmen
- Planung der einzelnen in der DS-GVO vorausgesetzten Prozesse,
- z.B.:
    - Zweckfestlegung und Zweckänderung
    - Verarbeitungsverzeichnis
    - Datensicherheit
    - "Privacy by design und by default"
    - Recht auf Datenübertragbarkeit
    - Reaktionsmechanismen auf Datenverletzungen
    - Informationspflichten bei Datenerhebung
    - Auskunftsrecht der betroffenen Person
    - Löschkonzepte
    - Recht auf Vergessenwerden
    - Recht auf Einschränkung der Verarbeitung
    - Widerspruchsrecht
    - Recht auf Berichtigung
    - Datenschutz-Folgenabschätzung
    - Gemeinsam Verantwortliche
    - Auftragsverarbeitung
    - Prozesse zu Profiling
    - Prozesse zu Big Data
    - Übermittlung von Daten in Drittstaaten
- Einrichtung eines effektiven und risikoangemessenen Beschwerdemanagements
- Vertragsmanagement
- Einwilligungsmanagement
- Dokumentation sämtlicher relevanter Prozesse[656]

655 *Wybitul, RA, Tim, / Draf, Dr. Oliver, LL.M.* Betriebsbs-Berater 2016.
656 *Wybitul, RA, Tim, / Draf, Dr. Oliver, LL.M.* Betriebsbs-Berater 2016 (S. 2101).

2.1.4.1 Projektteam

Der erste Prozessschritt zur Umsetzung der Verordnung war die Zusammenstellung eines Projektteams. Bei größeren oder datenintensiven Unternehmen war sogar an den Aufbau eines entsprechenden Project Management Office zu denken. Die Beteiligten sollten die Datenverarbeitungen in den unterschiedlichen betroffenen Bereichen sowie deren Zweck gut kennen und bereichsspezifische Anforderungen bei der Einführung der DS-GVO beachten und umsetzen können.

Neben der Datenschutzfunktion und den operativ tätigen Unternehmensbereichen kamen insbesondere Funktionen aus den Bereichen IT, Personal, Recht, Revision und Compliance in Betracht. Bei der Festlegung der Teilnehmer des Projektteams sollte darüber hinaus ebenfalls bestimmt werden, wer gegenüber der Unternehmensführung über Anforderungen und Fortgang des Implementierungsprojekts berichtet. Zudem sollte bei Unternehmensgruppen auch die „Konzernweite Brille" bei der Umsetzung sichergestellt sein. Das Projektteam sollte dann gegebenenfalls auf Konzernebene arbeiten und so die konzernweit einheitliche Umsetzung der Standards sicherstellen. Eine den Anforderungen des Unternehmens (oder des Konzerns) und der jeweiligen Projektphase entsprechende Zusammensetzung des Projektteams sollte kontinuierlich überprüft und bei Bedarf angepasst werden.[657]

2.1.4.2 Ressourcenplanung

Die Umsetzung der DS-GVO der Unternehmen erfordert gerade bei mittleren und größeren Unternehmen eine durchdachte risikoorientierte und professionelle Ressourcenplanung. Dabei gilt es insbesondere, nicht „das Rad neu zu erfinden". Vielmehr sollten Unternehmen unbedingt prüfen, auf welche bereits bestehenden Prozesse, Strukturen und sonstige Ressourcen sie bei der Einführung der DS-GVO zurückgreifen können. Zur Einführung eines effektiven Datenschutz Management Systems sind eine Vielzahl von Ablaufen und Strukturen zu koordinieren. Hier kann es ausgesprochen zweckmäßig sein, gerade in Bezug auf die Projektplanung und deren Steuerung, frühzeitig entsprechende Ressourcen sicherzustellen.[658]

---

657 *Wybitul, RA, Tim, / Draf, Dr. Oliver, LL.M.* Betriebsbs-Berater 2016 (S. 2102).
658 *Wybitul, RA, Tim, / Draf, Dr. Oliver, LL.M.* Betriebsbs-Berater 2016 (S. 2102).

2.1.4.3 Budgetplanung

Die Einführung der DS-GVO ist ein Projekt von erheblicher (auch finanzieller) Tragweite. Dies gilt sowohl für Geschäftsprozesse als auch für die Software als Supportprozess. Die effektive Implementierung eines nach Art. 24 Abs. I DS-GVO vorgeschriebenen und auch zur Vermeidung von Haftungsrisiken unumgänglichen Datenschutz Management Systems führt zu einem erheblichen Bedarf an personellen, organisatorischen und finanziellen Ressourcen. Bereits vor der Verabschiedung der Verordnung benötigte ein effektives Datenschutzprogramm ein angemessenes Budget. Die Anforderungen an Datenschutz Management Systeme steigen mit der Einführung der DS-GVO weiter. Daher sollten Budgetfragen bereits am Anfang des Einführungsprojekts angemessen berücksichtigt und über Vorstudien und Teilziele schrittweise präzisiert werden. Bei der Festlegung erforderlicher Budgets sollte das Unternehmen auch die drohenden Bußgelder von bis zu vier Prozent des globalen konzernweiten Umsatzes sowie bis zu Mio. Euro für Manager und andere für Datenschutzentscheidungen verantwortliche Personen, bedenken. Erfahrungsgemäß ist es zweckmäßig, sich hierzu auch mit anderen Unternehmen in ähnlicher (datenschutzrechtlicher) Gefährdungssituation oder auf der Ebene von Branchenverbanden abzustimmen.[659]

2.1.4.4 Risikoanalyse DS-GVO

Gerade aufgrund der erheblich gestiegenen Bußgeld- und Reputationsrisiken sowie künftig drohender Schadensersatzforderungen betroffener Personen ist eine auf das gesamte Unternehmen und dessen einzelne Bereiche bezogene Risikoanalyse nötig. Dabei sollten bestehende Risiken identifiziert und nach ihrer Eintrittswahrscheinlichkeit und dem Ausmaß nachteiliger Folgen sowie Möglichkeiten zur Risikovermeidung oder -Verringerung bewertet werden. Zudem setzen viele Vorschriften der Verordnung eine umfassende Risikoanalyse voraus. Beispielsweise müssen Unternehmen in Bezug auf die zu treffenden technischen und organisatorischen Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus bei der Datensicherheit die

659 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 112, Rn. 326+327.

„Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen" berücksichtigen, Art. 32 Abs. 1 DS-GVO.[660] [661]

Hierbei müssen Unternehmen logisch zwischen den (unmittelbaren) Risiken für die Rechte und Freiheiten von Personen und den daraus folgenden (mittelbaren) Konsequenzen möglicher Datenschutzverstöße für das Unternehmen selbst trennen. Beides sind Kriterien, die Unternehmen im Rahmen einer auf den Datenschutz bezogenen Risikoanalyse berücksichtigen müssen.[662]

Unternehmen sollten bei der Bewertung der konkret zu berücksichtigenden Risiken insbesondere die nachstehenden Aspekte berücksichtigen:[663]

2.1.4.5 Risiken für betroffene Personen

Ausgangspunkt jeder Risikoanalyse in Bezug auf den Datenschutz sind die möglichen Auswirkungen einzelner Datenverarbeitungen in Bezug auf von dieser Verarbeitung betroffenen Personen. Mögliche Eingriffe in die Rechte und Freiheiten dieser betroffenen Personen sind nach den Kriterien der Eintrittswahrscheinlichkeit und der zu erwartenden Eingriffsintensität näher zu bestimmen.[664]

2.1.4.5.1 Mögliche Bußgelder

Das für das Unternehmen beziehungsweise den Konzern geltende Maximalbußgeld pro Verstoß ist auf der Grundlage des Umsatzes des Vorjahres zu berechnen. Dabei ist auch an eine nach wie vor mögliche Gewinnabschöpfung zu denken.[665]

660 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 32 Abs. 1 DSGVO.

661 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 113, Rn. 328.

662 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 113, Rn. 329.

663 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 113, Rn. 330.

664 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 113, Rn. 331.

665 *Faust/Spittka/Wybitul*, Milliardenbußgelder nach der DS-GVO? Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz, in Zeitschrift für Datenschutz, S. 105.

Die Voraussetzungen für die Verhängung der Bußgelder nach Art. 53 Abs. 1b lit. g DS-GVO und Art. 58 Abs. 1 lit. i DS-GVO sowie für die Bestimmung der Höhe sind in Art. 79 DS-GVO, bzw. Art. 83 DS-GVO[666] geregelt.[667]

Die Bußgeldtatbestände des Art. 79 DS-GVO, Art. 83 DS-GVO umfassen eine Vielzahl von Pflichten, welche Unternehmen nach der DS-GVO treffen.

In Art. 79 Abs. 3 DS-GVO, Art. 83 Abs. 4 DS-GVO aufgeführte Verstöße können mit einem Bußgeld von bis zu € 10 Mio. oder im Fall eines Unternehmens 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs geahndet werden. Die übrigen Verstöße nach Abs. 3a und 3aa [= Art. 83 Abs. 5 und 6 DS-GVO] können zu Geldbußen von bis zu € 20 Mio. oder im Fall eines Unternehmens bis zu 4 % des Jahresumsatzes führen. In beiden Fällen gilt für Unternehmen, dass das umsatzbasierte Bußgeld die Grenzen von € 10 bzw. 20 Mio. übersteigen kann, wenn ein umsatzbezogenes Bußgeld zu einem höheren Betrag führt. Die DS-GVO sieht übrigens keine Deckelung auf einen bestimmten Höchstbetrag vor.[668]

Nachfolgende Abbildung 6 zeigt die relevanten Artikel der Datenschutz-Grundverordnung auf, die als Folge eine Geldbuße[669] mit sich bringen werden. Ein Verstoß gegen diese Artikel der Datenschutz-Grundverordnung kann mit Geldbußen von bis zu 10 Mio. Euro oder 2 % des Umsatzes des Vorjahres, geahndet werden.

666 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).

667 *Faust/Spittka/Wybitul*, Milliardenbußgelder nach der DS-GVO? Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz, in Zeitschrift für Datenschutz, S. 105.

668 *Faust/Spittka/Wybitul*, Milliardenbußgelder nach der DS-GVO? Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz, in Zeitschrift für Datenschutz, S. 105.

669 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), siehe Art. 82 und 83 DSGVO.

Abbildung 6: Geldbußen nach Art. 82 und Art. 83 DS-GVO[670]

2.1.4.5.2 Zivilrechtliche Haftungsrisiken

Unter zivilrechtlicher Haftung bzw. Haftungsrisiken ist die Berücksichtigung der möglichen Geltendmachung auch immaterieller Schäden nach Art. 82 Abs. 1 DS-GVO[671] sowie des Risikos von Verbandsklagen nach Art. 80 DS-GVO zu verstehen.[672]

670 *Reimann/e.V.,* Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung, 2. Aufl. 2018, S. 141.

671 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 82 Abs. 1 DSGVO.

672 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 114, Rn. 333.

2.1.4.5.3 Rufschäden

Erfahrungsgemäß können Fehler beim Datenschutz zu erheblichen Risiken für die Reputation eines Unternehmens führen. Auch dies ist im Rahmen einer umfassenden Gefährdungsanalyse zu berücksichtigen. Gerade für Kunden gewinnen Fragen des Datenschutzes zunehmend an Bedeutung.[673]

2.1.4.5.4 Arbeitsrechtliche Aspekte

Unternehmen sollten auch an mögliche Streitigkeiten mit dem Betriebsrat oder einzelnen Arbeitnehmern wegen möglichen Defiziten beim Datenschutz am Arbeitsplatz denken. Bei vielen Unternehmen ist der Datenschutz bei Verhandlungen mit Betriebsraten bereits jetzt ein Dauerthema. Es spricht sehr viel dafür, dass auch Betriebsräte und Gewerkschaften die Bedeutung der DS-GVO[674] erkennen und sich intensiver mit Fragen des Datenschutzes im Betrieb befassen werden.[675]

2.1.4.5.5 Sonstige Nachteile

Neben den vorstehenden Punkten sind auch sonstige mögliche Nachteile, wie etwa die Untersagung einzelner Datenverarbeitungen durch die zuständige Aufsichtsbehörde zu berücksichtigen.[676]

2.1.4.5.6 Bestandsaufnahme

Bei der Umsetzung der Vorgaben der Verordnung sollte das Projektteam grundsätzlich prüfen, auf welche bereits bestehenden Strukturen das Unternehmen aufsetzen kann. Wegen des gegenüber dem BDSG[677] deutlich stärker risikobasierten Ansatzes der Verordnung kommen hier neben der Nutzung bestehender Datenschutzstrukturen insbesondere auch die Übertragung oder Adaption von Prozessen sowie Maßstäben aus Compliance-Management-Systemen und dem Risikomanagement in Betracht.[678]

673 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 114, Rn. 334.
674 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).
675 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 114, Rn. 335.
676 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 114, Rn. 336.
677 Bundesdatenschutzgesetz, BDSG - Bundesdatenschutzgesetz.
678 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 114, Rn. 337.

2.1.4.5.7 Gap-Analyse (Lückenanalyse)

Grundsätzlich kann die Gap-Analyse als „Lückenanalyse“ definiert werden. Sie zeigt die strategische Lücke auf, indem sie den Unterschied zwischen den strategischen Zielen und der aktuellen Unternehmensprognose herausstellt.[679]

Bei der Gap-Analyse (Gap = Lücke) wird die gewünschte Entwicklung einer Zielgröße (z.B. Umsatz oder Gewinn) dem Verlauf dieser Größe gegenüber gestellt, der bei der derzeitigen Strategie erwartet wird. Die Abweichung zwischen beiden Entwicklungen offenbart eine strategische Lücke und deutet auf die Notwendigkeit einer Strategieänderung/-anpassung hin (z.B. Entwicklung und Einführung neuer Produkte).[680]

Das Unternehmen sollte im Rahmen der Umsetzung der Anforderungen der Verordnung einen strukturierten Abgleich des derzeitigen Ist-Zustands mit dem künftigen Soll-Zustand vornehmen. Auf dieser Grundlage lässt sich bereits eine erste Grobrasterung der einzelnen notwendigen Projektschritte erstellen. Damit ist die Gap-Analyse auch ein wichtiger Baustein in der weiteren Projektplanung, etwa in Bezug auf die Maßnahmen zur Gewährleistung der vorgeschriebenen Transparenz und Dokumentation. Konkret konnten in einem ersten Schritt der Umsetzung. der Gap-Analyse beispielsweise alle von der DS-GVO betroffenen Organisationseinheiten, Prozesse und rechtlichen Einheiten identifiziert werden.[681]

679 *Wirtschaftsanalyse24.com,* Gap-Analyse, http://www.wirtschaftslexikon24.com/d/gap-analyse-lueckenanalyse/gap-analyse-lueckenanalyse.htm.

680 *Wirtschaftsanalyse24.com,* Gap-Analyse, http://www.wirtschaftslexikon24.com/d/gap-analyse-lueckenanalyse/gap-analyse-lueckenanalyse.htm.

681 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 114, Rn. 338.

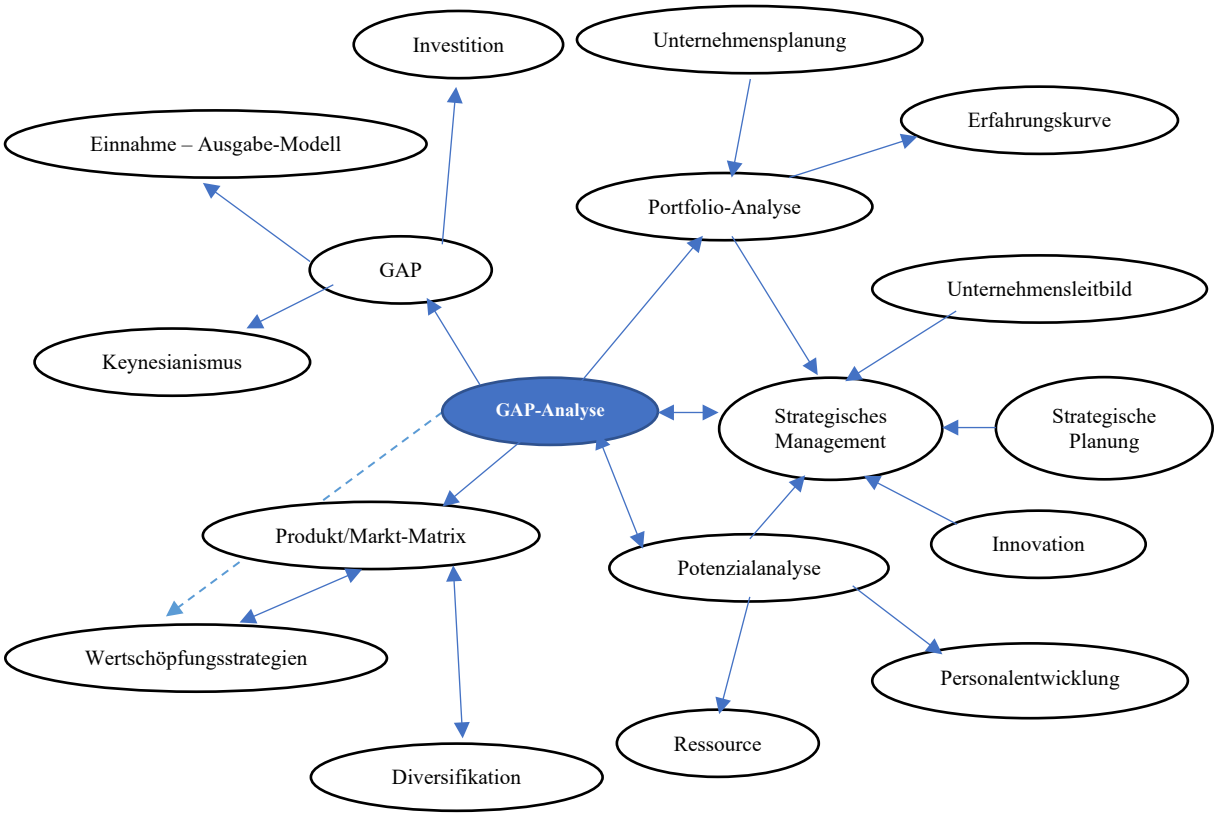

Abbildung 7: GAP-Analyse[682]

2.1.4.5.8 Einbindung Datenschutzbeauftragter

Der Datenschutzbeauftragte übernimmt sowohl bei der Einführung der in der DS-GVO[683] geforderten Strukturen als auch beim Betrieb des Datenschutz Management Systems eine zentrale Rolle. Er muss zudem „ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden" sein. Das Unternehmen sollte die Umsetzung dieser Anforderung auch in einer Art. 24 Abs. 1 DS-GVO entsprechenden Weise dokumentieren.[684]

682 In Anlehnung an Grafik Gap-Analyse, https://wirtschaftslexikon.gabler.de/definition/gap-analyse-34738.

683 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).

684 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 115, Rn. 340.

Der betriebliche Datenschutzbeauftragte berichtet gemäß Art. 38 Abs. 3 S. 3[685] unmittelbar an die höchste Managementebene. Diese Ansiedlung des Datenschutzbeauftragten in der personellen Unternehmensstruktur soll zum einen seine **Weisungsfreiheit** sichern und zum anderen das Thema Datenschutz nah an der Geschäftsleitung verankern. Die unmittelbare Anbindung an die höchste Managementebene verschafft ihm eine Position außerhalb der Unternehmenshierarchie. Er hat damit in dieser Funktion keine direkten Vorgesetzen, was ihm fachliche Unabhängigkeit sichert.[686]

2.1.4.5.9 Datenschutzkommunikation

Viele Unternehmen messen dem Datenschutz nach den Vorgaben der Verordnung einen höheren Stellenwert zu als nach dem bislang geltenden BDSG.[687] Die Implementierung und der Betrieb effektiver Datenschutz Management Strukturen setzen auch ein klares Bekenntnis der Unternehmensführung zum Datenschutz sowie eine unmissverständliche Kommunikation hierzu gegenüber der Belegschaft voraus. Dies umfasst gerade bei größeren Unternehmen auch geeignete Datenschutzrichtlinien.[688]

2.1.4.5.10 Datenschutztrainings

Die Anforderungen der DS-GVO sind komplex und vielfältig. Zur belastbaren Umsetzung der Vorgaben der Verordnung müssen Mitarbeiter gründlich geschult werden, insbesondere vor dem Hintergrund von Art. 24 Abs. 1 und Abs. 2 DS-GVO. Ferner fordert Art. 39 Abs. 1 lit. b DS-GVO ausdrücklich die „Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiterinnen und Mitarbeiter" durch den Datenschutzbeauftragten.[689]

Welcher Mitarbeiter auf welche Weise geschult werden muss, hängt von seiner jeweiligen Funktion und von seinen Aufgaben im Unternehmen ab. Dabei sollte das Unternehmen,

685 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 38 Abs. 3 S. 3 DSGVO.

686 *Forgó/Helfrich/Schneider* (Hrsg.), Betrieblicher Datenschutz, Betrieblicher Datenschutzbeauftrager, Teil II, Kapitiel 3, S. 227, Rn. 58.

687 Bundesdatenschutzgesetz.

688 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 115, Rn. 341.

689 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 115, Rn. 342.

die bei der Einführung und dem späteren Dauerbetrieb eines der DS-GVO[690] angemessenen Datenschutz Management Systems festgelegten Trainingskonzepte und deren Umsetzung auch in geeigneter Form dokumentieren. Hier bieten sich Branchenlösungen an, um sowohl Kosten zu sparen als auch gegebenenfalls enge finanzielle Umsetzungsrahmen einzuhalten.[691]

2.1.4.5.11 Datenschutzberatung

Eine solche Beratungspflicht gegenüber den Verantwortlichen findet sich in den neuen Datenschutzregelungen nicht mehr ausdrücklich. Die DS-GVO sieht in Art. 58 Abs. 3 lit. a lediglich die Beratung von Verantwortlichen vor, wenn diese sich i.R.v. Art. 36 im Hinblick auf eine Datenschutz-Folgenabschätzung vorab an die Aufsichtsbehörde wenden. Desgleichen normiert Art. 57 Abs. 1 lit. c DS-GVO[692] eine Beratungspflicht nur gegenüber dem Parlament, der Regierung und anderen (vergleichbaren) Einrichtungen und Gremien. Und auch das neue BDSG kennt in § 40 Abs. 6 nur noch die Beratung der Datenschutzbeauftragten, die Beratung der verantwortlichen Stellen ist hingegen gestrichen worden.[693]

Zutreffend ist auf den ersten Blick auch das Argument, eine Beratungspflicht könne schon deswegen nicht bestehen, weil angesichts der Vielzahl von Verantwortlichen im Wirkungsbereich der Aufsichtsbehörde und der Breite der möglichen Datenschutzfragen jede Aufsichtsbehörde durch einen entsprechenden Beratungsanspruch notwendig überfordert würde. Letztlich überzeugt aber auch dies nicht: Wollte man Rechtspflichten nur „nach Kassenlage“ der Aufsichtsbehörden akzeptieren, dann würde angesichts der prekären Ausstattung der großen Mehrzahl der Aufsichtsbehörden überhaupt keine der ausdrücklich in der DS-GVO verankerten Pflichten der Datenschutzbehörden wirksam sein.[694]

---

690 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).

691 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 115, Rn. 343.

692 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 57 Abs. 1 lit. c DS-GVO.

693 *Brink* ZD / Zeitschrift für Datenschutz Heft 2, 57.

694 *Brink* ZD / Zeitschrift für Datenschutz Heft 2, 57.

Der Datenschutzbeauftragte ist verpflichtet, das Unternehmen und die datenverarbeitenden Beschäftigten in Fragen des Datenschutzes zu beraten. Neben der Erfüllung dieser rechtlichen Pflicht ist die Einrichtung einer im Unternehmen gut kommunizierten und akzeptierten Datenschutzberatung ein wichtiges Mittel, um Fehler bei der Verarbeitung personenbezogener Daten und daraus folgende Risiken für das Unternehmen und die beteiligten Entscheidungsträger zu vermeiden.[695]

2.1.4.5.12 Information und Abstimmung mit den Datenschutzbehörden

Nach Art. 39 Abs. 1 lit. d DS-GVO[696] zählt die Zusammenarbeit mit den Aufsichtsbehörden zu den gesetzlich geregelten Aufgaben des Datenschutzbeauftragten. Beim Auftreten eines Datenschutzverstoßes ist der Verantwortliche nach Art. 33 Abs. 1 DS-GVO[697] verpflichtet, die zuständige Aufsichtsbehörde zu informieren, es sei denn, dass die Verletzung nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. In der Praxis bietet es sich an, dass der Datenschutzbeauftragte diese Information der Aufsichtsbehörde koordiniert und durchführt. In jedem Fall sollten die Zuständigkeiten, Berichtswege und die nötige interne Freigabe für die Kontaktaufnahme mit Datenschutzbehörden im Unternehmen klar geregelt sein.[698]

2.1.4.5.13 Betriebsrat und Betriebsvereinbarungen

Betriebsräte haben über die Einhaltung der Vorschriften zum Schutz der Arbeitnehmer zu wachen. Die DS-GVO[699] zählt zu diesen Schutzvorschriften. Aus Arbeitgebersicht empfiehlt es sich dringend, zu Fragen der Umsetzung der Verordnung frühzeitig den Kontakt mit dem Betriebsrat zu suchen. Hier bietet sich gegebenenfalls sogar die Möglichkeit gemeinsamer Schulungen und Workshops an, insbesondere um unnötige Kontroversen bei der Ausgestaltung des Arbeitnehmerdatenschutzes im Rahmen der DS-

695 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 116, Rn. 344.

696 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 39 Abs. 1 lit. (d).

697 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 33 Abs. 1 DSGVO.

698 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 116, Rn. 345.

699 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).

GVO zu vermeiden. Die DS-GVO erfordert teilweise erhebliche Anpassungen bei bestehenden Betriebsvereinbarungen. Zudem kann auch der Abschluss neuer Betriebsvereinbarungen sehr zweckmäßig sein. Erfahrungsgemäß kann es gerade bei Datenschutzfragen beziehungsweise bei Leistungsgrund Verhaltenskontrollen nach § 87 Abs. 1 Nr. 6 BetrVG lange dauern, neue Betriebsvereinbarungen unter Dach und Fach zu bringen. Dies sollte das Projektteam bei der zeitlichen Planung des Einführungsprojekts berücksichtigen.[700]

2.1.4.6 Planung der in der DS-GVO geforderten Prozesse und Strukturen

Die Verordnung sieht eine ganze Reihe von (teilweise recht komplexen) Abläufen bzw. Strukturen vor, die Unternehmen bis Mitte 2018 umgesetzt haben mussten. Dabei sollte das Projektteam insbesondere die folgenden Anforderungen berücksichtigen und die zu ihrer Umsetzung notwendigen Prozesse planen:[701]

2.1.4.6.1 Zweckfestlegung

Bei der erstmaligen Erhebung oder sonstigen Verarbeitung personenbezogener Daten muss das Unternehmen die Zwecke festlegen, für die es diese Daten verarbeitet. Hierfür ist ein strukturierter Prozess erforderlich, der sicherstellt, dass die vorgeschriebene Zweckfestlegung auch tatsächlich vorgenommen und dokumentiert wird. Viele Unternehmen dokumentieren die Zweckfestlegung beispielsweise im Verarbeitungsverzeichnis und stellen durch entsprechende Kontroll- bzw. Genehmigungsverfahren sicher, dass diese Anforderung im Einzelfall nicht umgangen wird. Das Unternehmen muss die betroffenen Personen über die festgelegten Zwecke der Verarbeitung ihrer personenbezogenen Daten im Rahmen der Informationspflichten nach Art. 13 Abs. 1 lit. c oder Art. 14 Abs. 1 lit. c DS-GVO[702] informieren.[703]

2.1.4.6.2 Zweckänderung

Ebenso wie für die Zweckfestlegung sind auch für mögliche Zweckänderungen klare Prozesse erforderlich. Die Anforderungen für die Verarbeitung personenbezogener Daten

---

700 *Wybitul, RA, Tim, / Draf, Dr. Oliver, LL.M.* Betriebsbs-Berater 2016 (S. 2104).
701 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 117, Rn. 348.
702 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 13 Abs. 1 lit. (c) oder Art. 14 Abs. 1 lit. (c) DSGVO.
703 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 117, Rn. 349.

für einen anderen als den ursprünglich festgelegten Zweck ergeben sich aus Art. 6 Abs. 4 DS-GVO.[704] [705]

2.1.4.6.3 Verarbeitungsverzeichnis

Nach Art. 30 DS-GVO müssen Unternehmen ihre Datenverarbeitungen in einem Verarbeitungsverzeichnis dokumentieren. Das Verarbeitungsverzeichnis kann ein wichtiger Baustein im Rahmen einer umfassenden Dokumentation im Sinne von Art. 24 Abs. 1 DS-GVO sein.[706]

2.1.4.6.4 Datensicherheit

Das Unternehmen muss auf der Basis einer Risikoanalyse ein angemessenes Schutzniveau in Bezug auf die Sicherheit der Verarbeitung gewährleisten. Hierbei sollten Unternehmen insbesondere Möglichkeiten zur Pseudonymisierung und Verschlüsselung personenbezogener Daten prüfen, vgl. Art. 32 Abs. l lit. a DS-GVO.[707] [708]

2.1.4.6.5 Privacy by Design and by Default

Art. 25 DS-GVO[709] verpflichtet Verantwortliche dazu, den vorgeschriebenen Datenschutz auch durch die Gestaltung der von ihnen eingesetzten IT und durch datenschutzfreundliche Voreinstellungen umzusetzen. Unternehmen müssen die Datenschutzgrundsätze nach Art. 5 DS-GVO auch durch geeignete technische Maßnahmen umsetzen. Beispiele hierfür sind auf Datenminimierung ausgerichtete IT-Systeme und die möglichst umfassende und frühzeitige Pseudonymisierung personenbezogener Daten. Der Umfang der konkret zu treffenden Maßnahmen beruht auch hier auf einer Risikoanalyse.[710]

---

704 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 6 Abs. 4 DSGVO.

705 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 117, Rn. 351.

706 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 117, Rn. 352.

707 Datenschutz Grundverordnung vom 27.04.2016, Art. 32 Abs. l lit. (a) DSGVO.

708 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 118, Rn. 353.

709 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 25 DSGVO.

710 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 118, Rn. 354 + 355.

2.1.4.6.6 Recht auf Datenübertragbarkeit

Unternehmen sollten sicherstellen, dass sie das in Art. 20 DS-GVO normierte Recht auf Datenübertragbarkeit umsetzen können. Danach können betroffene Personen von Verantwortlichen verlangen, sie betreffende Daten „**in einem strukturierten, gängigen und maschinenlesbaren Format**" zu erhalten. Dies betrifft jedoch nur Daten, die dem Verantwortlichen zuvor von der betroffenen Person bereitgestellt wurden. Nach Art. 20 Abs. 2 DS-GVO kann die betroffene Person auch eine direkte Übermittlung an einen anderen Verantwortlichen verlangen, soweit dies technisch machbar ist. Da das Recht auf Datenübertragbarkeit nicht auf Kunden beschränkt ist, sollten sich Verantwortliche künftig auch auf entsprechende Forderungen von Mitarbeitern oder Geschäftspartnern einstellen. Die Umsetzung dieser Anforderung kann in Unternehmen einen erheblichen organisatorischen, technischen und wirtschaftlichen Aufwand erfordern.[711]

2.1.4.6.7 Reaktionsmechanismen auf Datenverletzungen

Unternehmen sollten auch Maßnahmen zur Verringerung der Folgen einer Verletzung des Schutzes personenbezogener Daten, Strukturen zur Meldung bei der Aufsichtsbehörde und zur gegebenenfalls erforderlichen Benachrichtigung betroffener Personen umsetzen.[712]

2.1.4.6.8 Informationspflichten bei Datenerhebung

Insgesamt sieht die DS-GVO ein deutlich höheres Maß an Transparenz vor als bislang das BDSG.[713] Gerade für die Information betroffener Personen sollten Unternehmen entsprechende Strukturen und Prozesse schaffen und dokumentieren. So sehen etwa Art. 13 und Art. 14 DS-GVO[714] umfassende Mitteilungspflichten bei der Erhebung personenbezogener Daten vor.[715]

2.1.4.6.9 Auskunftsrecht der betroffenen Person

Nach Art. 15 DS-GVO[716] haben betroffene Personen künftig umfassendere Auskunftsrechte als bislang nach § 34 BDSG.[717] Unter anderem muss das Unternehmen der betroffenen Person eine Kopie aller personenbezogenen Daten zur Verfügung stellen,

711 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 118, Rn. 356.
712 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 118, Rn. 357.
713 Bundesdatenschutzgesetz.
714 Datenschutz Grundverordnung vom 27.04.2016.
715 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 118, Rn. 358.
716 Datenschutz Grundverordnung vom 27.04.2016, Art. 15 DSGVO.
717 Bundesdatenschutzgesetz, § 34 BDSG.

die diese Person dem Verantwortlichen bereitgestellt hat. Zur Erfüllung dieser gesetzlichen Anforderung ist eine intensive Einbindung der IT-Verantwortlichen notwendig.[718]

2.1.4.6.10 Löschkonzepte

Wie schon nach dem BDSG müssen Unternehmen auch nach der Verordnung angemessene Löschkonzepte erstellen und umsetzen. Hier ist zunächst eine präzise Prüfung der Anforderungen nach Art. 17 DS-GVO in Bezug auf die im Unternehmen jeweils verarbeiteten Daten und die damit verfolgten Zwecke geboten. Die DS-GVO fordert die Festlegung von Löschfristen oder Löschkonzepten auch an anderer Stelle. Wenn Verantwortliche, betroffene Personen über die Erhebung ihrer personenbezogenen Daten informieren, müssen sie die betroffenen Personen auch über die Dauer der Speicherung ihrer Daten unterrichten. Nur falls eine derart genaue Unterrichtung nicht möglich ist, kann es ausreichen, die Kriterien für die Festlegung dieser Dauer mitzuteilen.[719]

2.1.4.6.11 Recht auf Vergessenwerden

Sofern Unternehmen personenbezogene Daten veröffentlichen, müssen sie auch sicherstellen, dass sie das in Art. 17 Abs. 2 DS-GVO vorgeschriebene „Recht auf Vergessenwerden" („right to be forgotten“) umsetzen. Dafür müssen Unternehmen angemessene Maßnahmen treffen, um andere Verantwortliche, die diese öffentlich gemachten Daten verarbeiten, entsprechend über das Vorliegen eines Löschgrundes zu informieren. Die Information anderer Verantwortlicher muss beinhalten, dass die betroffene Person die Löschung aller Links zu ihren personenbezogenen Daten oder von Kopien dieser Daten verlangt hat. Auch die Umsetzung dieses Rechts in die Praxis erfordert einige Vorbereitung.[720]

2.1.4.6.12 Recht auf Einschränkung der Verarbeitung

Betroffene Personen können verlangen, dass der Verantwortliche ihre personenbezogenen Daten nur noch für eingeschränkte Zwecke verarbeitet, sofern eine

718 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 119, Rn. 359.
719 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 119, Rn. 360.
720 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 119, Rn. 361.

der in Art. 18 Abs. 1 DS-GVO[721] aufgezählten Voraussetzungen vorliegt. Auch für die Bearbeitung derartiges Verlangen muss das Unternehmen angemessene Prozesse installieren.[722]

2.1.4.6.13 Widerspruchsrecht

Art. 21 DS-GVO sieht das Recht betroffener Personen vor, der Verarbeitung ihrer personenbezogenen Daten zu widersprechen. Der Verantwortliche muss die betroffene Person spätestens zum Zeitpunkt der ersten Kommunikation mit ihr auf dieses Widerspruchsrecht hinweisen, Art. 21 Abs. 4 DS-GVO. Macht die betroffene Person von ihrem Recht zum Widerspruch Gebrauch, muss das Unternehmen die Daten gegebenenfalls „einschränken" und darf sie bis auf weiteres nur noch für die in Art. 18 Abs. 2 DS-GVO genannten Zwecke verarbeiten. Im Anschluss muss das Unternehmen prüfen, ob die Voraussetzungen eines Verarbeitungsverbots nach Art. 21 Abs. 1 DS-GVO vorliegen.[723]

2.1.4.6.14 Recht auf Berichtigung

Nach Art. 16 DS-GVO kann eine betroffene Person verlangen, dass der Verantwortliche unrichtige personenbezogene Daten über sie unverzüglich berichtigt und gegebenenfalls auch vervollständigt. Dies setzt ein Verfahren voraus, mit dem das Unternehmen überprüfen kann, ob die in Frage stehenden personenbezogenen Daten tatsächlich unrichtig sind.[724]

2.1.4.6.15 Auftragsverarbeitung

Bis zur unmittelbaren Geltung der Verordnung am 25. Mai 2018 sollten Verantwortliche sichergestellt haben, dass die Verträge mit den von ihnen eingesetzten

721 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 18 Abs. 1 DSGVO.

722 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 119, Rn. 362.

723 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 120, Rn. 363.

724 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 120, Rn. 364.

Auftragsverarbeitern den Anforderungen von Art. 28 und Art. 29 DS-GVO[725] entsprechen.[726]

2.1.4.6.16 Profiling

Das automatisierte Erstellen von Persönlichkeitsprofilen ist nach Art. 22 DS-GVO an hohe Anforderungen geknüpft, sofern betroffene Personen auf der Grundlage ausschließlich automatisierter Verarbeitung „Entscheidungen unterworfen" werden. Unternehmen sollten prüfen, ob und in welcher Form sie Profiling künftig noch einsetzen dürfen.[727]

2.1.4.6.17 Prozesse zu Big Data

Die Verordnung gilt auch beim Einsatz von **Big Data**. Gerade bei weitgehenden Verarbeitungen sehr großer Datenmengen dürfte es für Unternehmen teilweise schwierig werden, die in Art. 13 ff. DS-GVO geforderten Transparenzanforderungen sowie die weiteren Vorgaben der Verordnung umzusetzen. Hier sollten Verantwortliche prüfen, in welchen Unternehmensbereichen **Big Data** überhaupt zum Einsatz kommt und ob gegebenenfalls die Verarbeitung pseudonymisierter oder sogar anonymisierter Daten möglich und zweckmäßig ist.[728]

2.1.4.6.18 Übermittlung von Daten in Drittstaaten

Unternehmen sollten personenbezogene Daten nur dann in Drittstaaten außerhalb der EU ohne angemessenes Datenschutzniveau übermitteln, wenn durch entsprechende Prozesse und Genehmigungsverfahren sichergestellt ist, dass die fraglichen Übermittlungen den Anforderungen der Art. 44 ff. DS-GVO[729] entsprechen.[730]

---

725 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 28 und Art. 29 DSGVO.

726 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 121, Rn. 368.

727 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 121, Rn. 369.

728 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 121, Rn. 370.

729 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 44 ff. DSGVO.

730 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 121, Rn. 371.

2.1.4.7 Beschwerdemanagement

Die Umsetzung des Rechts auf eingeschränkte Datenverarbeitung und anderer Betroffenenrechte legt es nahe, dass Unternehmen ein entsprechendes „Beschwerdemanagement“ einrichtet, mit dem es auf die Geltendmachung von Ansprüchen auf Auskunft (Art. 15 DS-GVO),[731] Berichtigung (Art. 16 DS-GVO), Löschung und „Vergessenwerden“ (Art. 17 DS-GVO), Einschränkung (Art. 18 DS-GVO), Datenübertragung (Art. 20 DS-GVO), die Geltendmachung des Widerspruchsrechts (Art. 21 DS-GVO) und sonstige Beschwerden reagieren kann.[732]

2.1.4.8 Vertragsmanagement

Unternehmen sind gut beraten, bereits geltende und noch abzuschließende Verträge und deren Regelungsinhalte darauf zu prüfen, ob sie den Anforderungen der Verordnung entsprechen oder ob sie angepasst werden müssen. Dies gilt insbesondere für Verträge über Auftragsverarbeitung oder die Übermittlung von personenbezogenen Daten, aber auch für sonstige Verträge, welche die Verarbeitung personenbezogener Daten betreffen.[733]

2.1.4.9 Einwilligungsmanagement

Art. 6 Abs. 1 lit. a DS-GVO knüpft vergleichsweise hohe Anforderungen an die Einwilligungen betroffener Personen in die Verarbeitung ihrer personenbezogenen Daten. Daher empfiehlt es sich, strukturiert zu prüfen (und zu dokumentieren), an welchen Stellen im Unternehmen personenbezogene Daten derzeit auf der Grundlage von Einwilligungen verarbeitet werden und die entsprechenden Prozesse und Verarbeitungen von § 4a BDSG[734] auf Art. 7 DS-GVO[735] zu stellen.[736]

---

731 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).

732 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 121, Rn. 372.

733 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 121, Rn. 373.

734 Bundesdatenschutzgesetz, § 4a BDSG.

735 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 7 DSGVO.

736 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 122, Rn. 374.

2.1.4.10 Dokumentation

Art. 24 Abs. 1 DS-GVO stellt sehr hohe Anforderungen an die Dokumentation bestehender Datenschutz Prozesse im Unternehmen. Auch wegen der dort vorgesehenen Beweislastregelung sollten Unternehmen ihr Datenschutz Management System nebst den damit verbundenen Prozessen und Strukturen umfassend dokumentieren. Andernfalls wird es dem Unternehmen nicht möglich sein, den in Art. 24 Abs. 1 und Art. 5 Abs. 2 DS-GVO geforderten Nachweis dafür zu erbringen, dass seine Datenverarbeitungen gemäß der Verordnung erfolgen. Eine Herausforderung für das Umsetzungsprojekt zur Einführung der DS-GVO dürfte es sein, die Dokumentationspflicht im Unternehmen beziehungsweise im Konzern und, wo sinnvoll, auch in einzelnen Geschäftsbereichen einheitlich umzusetzen.[737]

737 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 122, Rn. 375.

2.2 Benennung Datenschutzbeauftragter

Bis zu ihrer Einführung in die DS-GVO[738] war die Pflicht zur Benennung eines Datenschutzbeauftragten in **den meisten EU-Mitgliedstaaten weitgehend unbekannt**. Die obligatorische Benennung eines Datenschutzbeauftragten wird allerdings im deutschen Datenschutzrecht bereits seit mehr als 30 Jahren vorgeschrieben und hat sich als Erfolgsmodell erwiesen. Im Rahmen der DS-GVO wird der Datenschutzbeauftragte eine Schlüsselrolle im Hinblick auf die Einhaltung der Vorgaben der Verordnung spielen.[739]

Die Benennung eines Datenschutzbeauftragten gehört zu den essenziellen Themen in Bezug auf die Einführung der Datenschutz-Grundverordnung. Das Unternehmen hatte bereits in der Vergangenheit (vor der Einführung der Datenschutz-Grundverordnung) eine Pflicht zur Benennung eines Datenschutzbeauftragten. Dabei handelte es sich meiner Meinung nach eher um eine „Alibi-Benennung. Erst als die Einführung der Datenschutz-Grundverordnung zeitlich näher rückte, erhielt das Unternehmen die Kündigung der Beratungstätigkeit auf Grundlage des BDSG a.F. mit gleichzeitigem Hinweis auf die Einführung der DS-GVO und einem neuen Angebot zu geänderten Konditionen.

Die Entscheidung ob ein externer oder interner Datenschutzbeauftragter beauftragt bzw. benannt werden soll, musste folglich getroffen werden. Dabei sollte im Auftrag der Konzernleitung eine Kostenaufstellung angefertigt werden mit möglichen Vor- und Nachteilen. Zu beachten waren die rechtliche Situation und die Auflagen bezüglich des Datenschutzbeauftragten.

738 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).

739 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, S. 65, Abschnitt 3.6 Datenschutzbeauftragter.

Eine Verpflichtung zur Benennung (nicht länger „Bestellung“) eines **D**aten**s**chutz**b**eauftragten (**DSB**) besteht für Verantwortliche und Auftragsverarbeiter nach der DS-GVO nur in den sich aus Art. 37 Abs. 1 DS-GVO[740] sowie aus Art. 37 Abs. 4 DS-GVO i. V. m. §§ 5 Abs. 1, 38 Abs. 1 BDSG n.F.[741] ergebenden Fällen.[742]

Die Benennung muss schriftlich erfolgen und setzt ein beiderseitiges Einverständnis (also zwischen verantwortlicher Stelle und der Person des Datenschutzbeauftragten) voraus. Die ggf. zusätzlich erfolgende Aufgabenzuweisung hat zugleich Auswirkungen auf die arbeitsrechtliche Beziehung des Datenschutzbeauftragten. Gleichwohl kann ein Datenschutzbeauftragter auch außerhalb der verantwortlichen Stelle stehen (externer Datenschutzbeauftragter), ist jedoch im Rahmen seiner Tätigkeit Teil der verantwortlichen Stelle.[743]

Art. 37 DS-GVO regelt, in welchen Fällen eine Pflicht zur Benennung eines Datenschutzbeauftragten besteht. Sowohl der Verantwortliche als auch der Auftragsverarbeiter können von dieser Verpflichtung betroffen sein. Außerdem ermöglicht es Art. 37 Abs. 4 DS-GVO den EU-Mitgliedstaaten sowie der EU Rechtsvorschriften zu erlassen, die den Verantwortlichen, den Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, zur Benennung eines Datenschutzbeauftragten verpflichten.[744]

Nach Art. 37 Abs. 1 lit. b, c DS-GVO sind private Unternehmen zur Benennung eines Datenschutzbeauftragten in folgenden Fällen verpflichtet:

– Regelmäßige und systematische Überwachung: Die Kerntätigkeiten bestehen in der Durchführung von Verarbeitungsvorgängen, die aufgrund ihrer Art, ihres

740 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 37 Abs. 1 DS-GVO.

741 Bundesdatenschutzgesetz, neue Fassung BDSG - Bundesdatenschutz Gesetz.

742 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, Benennung als Datenschutzbeauftragter, S. 69, Satz 1.

743 *Witt,* Datenschutz kompakt und verständlich, 2008, S. 85, Abs. 2.

744 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, Pflicht zur Benennung, S. 66 3.6.1.

Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen.[745]

– Besondere Kategorien personenbezogener Daten: Die Kerntätigkeiten bestehen in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten oder von personenbezogenen Daten (Art. 9 Abs. 1 DS-GVO)[746] über strafrechtliche Verurteilungen und Straftaten.[747]

Die DS-GVO führt die Begriffe „**Kerntätigkeit**“ und „**umfangreich**“ nicht weiter aus, sodass das Ausmaß der Benennungspflicht einer genaueren Erläuterung bedarf. Sobald die Benennung stattgefunden hat, veröffentlicht der Verantwortliche/ Auftragsverarbeiter die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.[748] Da der Datenschutzbeauftragte als Anlaufstelle für betroffene Personen dienen soll, ist eine durchgängige Verfügbarkeit seiner Kontaktdaten sicherzustellen, bspw. durch Veröffentlichung auf der Website des Unternehmens..[749]

Auf Grundlage der vorliegenden Informationen wurde die Entscheidung getroffen einen externen Datenschutzbeauftragten zu benennen. Hierzu wurden unterschiedliche Angebote eingeholt, Gespräche geführt und nach Abwägung den aktuell noch zuständigen Datenschutzbeauftragten bzw. das Unternehmen benannt. Die damit verbunden Kosten erhöhten sich signifikant um mehrere 100 %. Diese Aufwendungen mussten künftig als Position in die Budgetplanung aufgenommen werden.

745 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, Pflicht zur Benennung, S. 66 3.6.1.

746 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 9 Abs. 1 DSGVO.

747 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, S. 66 Abs. 3.

748 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 37 Abs. 7 DSGVO.

749 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, DSGVO, Art. 37, Rn. 17.

Abschnitt 4

Datenschutzbeauftragter

Artikel 37

Benennung eines Datenschutzbeauftragten

(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn:

a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,

b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder

c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.[750]

750 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Abschnitt 4, Daatenschutzbeauftragter, Art. 37 Abs. 1 lit. a - c.

2.3 Schulungen der Mitarbeiterinnen und Mitarbeiter

Dem Datenschutzbeauftragten obliegt es darüber hinaus, die Mitarbeiter der verantwortlichen Stelle mit den gesetzlichen Bestimmungen des Datenschutzes vertraut zu machen. Aufgrund der rasanten Entwicklung im Bereich des Datenschutzes ist seine Schulungs- und Fortbildungsfunktion als Daueraufgabe zu begreifen.[751] Ziel dieser Schulung ist zum einen die Vermittlung datenschutzrechtlicher Grundkenntnisse sowie zum anderen die Sensibilisierung der Angestellten im Umgang mit personenbezogenen Daten.[752] Dabei sind die Schulungsmaßnahmen auf die Tätigkeit der verantwortlichen Stelle und auf die spezifischen Verarbeitungsvorgänge der jeweils aufzuklärenden Abteilungen abzustimmen.[753]

Mitarbeiter sind sich des Umgangs mit personenbezogenen Daten häufig nicht bewusst. Durch Unterweisungen und Schulungen ist sicherzustellen, dass Mitarbeiter über Folgendes informiert sind: [754]

- den Zweck des Bundesdatenschutzgesetzes bzw. der DS-GVO
- die Definition von personenbezogenen Daten
- die Bedeutung des Datengeheimnisses
- besondere Arten von personenbezogenen Daten
- die Bedeutung der Vorabkontrolle
- die Definition des Umgangs mit personenbezogenen Daten (Erhebung, Verarbeitung, Nutzung)
- die Grundsätze von Datenvermeidung, -sparsamkeit, -anonymisierung und Pseudonymisierung
- Auskunftsrechte
- Maßnahmen zur Datensicherheit und die Besonderheiten im Datenschutzrecht
- die Abgrenzung von Funktionsübertragung und Auftragsverarbeitung
- Straf- und Bußgeldvorschriften gemäß §§ 42 und 43 BDSG.[755]

---

751 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, § 4g BDSG, Rn. 16, 20.
752 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, § 4 BDSG, Rn. 21.
753 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, § 4 BDSG, Rn. 22.
754 *Reimann/e.V.,* Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung, 2. Aufl. 2018, Schulungen und Unterweisungen im Datenschutz, S. 134.
755 Bundesdatenschutzgesetz, §§ 42 und 43 BDSG.

Aus dieser Aufstellung der Forderungen an eine gute Unterweisung im Datenschutz ergibt sich gleichzeitig deren Gliederung. Ein praxisorientiertes und bewährtes „Merkblatt zur Verpflichtung auf das Datengeheimnis nach § 5 BDSG“ wurde durch den Forum Verlag herausgegeben.[756]

Neben der mündlich stattfindenden Unterweisung zu o. g. Themen im Datenschutz wird das Merkblatt jedem Mitarbeiter zur Verfügung gestellt. Ein Exemplar des Merkblatts wird vom Mitarbeiter unterzeichnet und in der Personalakte aufbewahrt. Das Merkblatt ist gemäß rechtlichen Änderungen zu aktualisieren. Ein Überwachungsrhythmus im Abstand von einem Jahr hat sich dabei in der Praxis bewährt. Im Rahmen der Unterweisung haben sich neben der Verwendung des Merkblatts auch Präsentationen durchgesetzt, die an den Mitarbeiter entweder ausgegeben werden oder über Intranet abrufbar sind.[757] Auch in diesem Fall soll auf die Überwachungs- und Aktualisierungspflicht hingewiesen werden.

Das Thema Datenschutz-Grundverordnung, wird wie bereits erklärt als sinnvoll und notwendig erachtet. Das Thema inhaltlich zu erfassen und zu verstehen steht auf einem anderen Blatt. Die erforderlichen Artikel der Datenschutz-Grundverordnung werden nur selten komplett erfasst und verstanden. Dieses gekoppelt an eine etwas langatmige Präsentation und schon ist eine geplante Schulung nicht mehr interessant.

Es gibt einige Ansätze die eine Datenschutz Schulung etwas weniger anstrengend wirken lässt. Die Online Seite, Datenschutzbeauftragter-Info.de hat hierzu einen interessanten Ansatz formuliert.

Datenschutzschulungen können langweilig sein und tatsächlich als unnötig empfunden werden. Richtig ist auch, dass Datenschutzschulungen mitunter kaum ernst genommen werden oder eine gewisse Sensibilität erst aufkommt, wenn es zu einem schwerwiegenden Datenschutzvorfall kommt. Andererseits sollten

756 *Reimann/e.V.,* Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung, 2. Aufl. 2018, Schulungen und Unterweisungen im Datenschutz, S. 134.

757 *Reimann/e.V.,* Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung, 2. Aufl. 2018, Schulungen und Unterweisungen im Datenschutz, S. 134.

Datenschutzschulungen wie aufgezeigt auch fester Bestandteil des Datenschutzmanagements im Unternehmen sein.[758]

Dabei müssen Datenschutzschulungen nicht langweilig sein. Diese können durch:

- spannende Vorträge
- unterhaltsame oder aktive E-Learning-Schulungen
- abwechslungsreiche Workshops
- interessante Fallstudien
- herausfordernde Tests oder
- Teambuildingmaßnahmen in Form von Plan-/Rollenspiele etc.,

alles andere als langweilig gestaltet werden.[759]

Gerade auch durch eine fachlich fundierte Schulung kann ebenfalls viel für das Gelingen einer Datenschutzschulung getan werden. Bei einer Grundschulung sollte inhaltlich ein erster Überblick zum Datenschutz gegeben werden. Dabei können insbesondere folgende Themenbereiche in Betracht kommen:

- Grundsätze des Datenschutzes
- Rechtlicher Rahmen und wesentliche Begriffe des Datenschutzes
- Grundlagen der Datenverarbeitung
- Betroffenenrechte
- Verhalten bei Datenschutzverletzungen und Verstößen
- Hinweise zu den technischen und organisatorischen Maßnahmen / zur Datensicherheit
- Hinweise zum datenschutzgerechten Einsatz mobiler Geräte
- Hinweise zur Datenschutzrichtlinie im Unternehmen[760]

---

758 *Datenschutzbeauftragter-info.de,* Datenschutzschulung – Mitarbeiter sensibilisieren, ohne zu langweilen, https://www.datenschutzbeauftragter-info.de/datenschutzschulung-mitarbeiter-sensibilisieren-ohne-zu-langweilen/.

759 *Datenschutzbeauftragter-info.de,* Datenschutzschulung – Mitarbeiter sensibilisieren, ohne zu langweilen, https://www.datenschutzbeauftragter-info.de/datenschutzschulung-mitarbeiter-sensibilisieren-ohne-zu-langweilen/.

760 *Datenschutzbeauftragter-info.de,* Datenschutzschulung – Mitarbeiter sensibilisieren, ohne zu langweilen, https://www.datenschutzbeauftragter-info.de/datenschutzschulung-mitarbeiter-sensibilisieren-ohne-zu-langweilen/.

Demgegenüber sollten Themenschulungen zu bestimmten Themen erfolgen, wie folgende Beispiele zeigen:

- Beschäftigtendatenschutz in der Personalabteilung
- Datenschutz & Marketing
- Datenschutz bei Einsatz risikoreicher Technologien etc.[761]

2.3.1 Unterweisungen

Unterweisungspflichten entstehen

- bei der Ersteinweisung von Mitarbeitern, die mit personenbezogenen Daten umgehen,
- bei der Einstellung von Aushilfen, Zivilarbeitskräften, Auszubildenden, Praktikanten,
- so nicht anders geregelt auch für Fremdfirmen (z. B. Dienstleister für Reinigung, Wartung von IT-Komponenten und Druck- und Kopiertechnik) und Besucher.[762]

Zur Sensibilisierung von Mitarbeitern und zur Aufrechterhaltung des betrieblichen Datenschutzes im Unternehmen empfehlen sich regelmäßige Schulungen, i. d. R. auf jährlicher Basis. Im Fokus dieser Schulungen sollen neben der Wiederholung der grundlegenden Unterweisungsthemen vor allem aktuelle Änderungen im Bundesdatenschutzgesetz und in anderen rechtlichen Rahmenbedingungen für den Datenschutz sowie in Rechtsprechungen, Veröffentlichungen in den Medien und aktuelle Themen stehen. Best-practice-Beispiele zeigen, dass die Beschäftigung mit dem Datenschutz keineswegs ein trockenes Thema sein muss. Mit etwas didaktisch-methodischem Geschick lassen sich Schulungen für den Datenschutz recht abwechslungsreich und interessant gestalten. Neben der allseits bekannten Power-Point-Präsentation zur Vermittlung von neuen Kenntnissen können Auszüge aus Gerichtsurteilen zur Diskussion stehen und Fallbeispiele aus der gelebten Praxis in Gruppenarbeit untersucht, bewertet und mit Lösungen versehen werden. Dazu empfiehlt

761 *Datenschutzbeauftragter-info.de,* Datenschutzschulung – Mitarbeiter sensibilisieren, ohne zu langweilen, https://www.datenschutzbeauftragter-info.de/datenschutzschulung-mitarbeiter-sensibilisieren-ohne-zu-langweilen/.

762 *Reimann/e.V.,* Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung, 2. Aufl. 2018, S. 134, 12.2 Unterweisungen.

sich die Bildung von Kleinstgruppen (2 – 3 Mitarbeiter), die an je einem Fallbeispiel arbeiten.[763]

2.3.2 Schulungsplan

Schulungen müssen geplant werden. Nicht immer ist es möglich, alle Mitarbeiter gleichzeitig zu schulen. Weiterhin sollte der unterschiedliche Grad im Umgang mit personenbezogenen Daten bei der Schulungsplanung berücksichtigt werden. In der Praxis durchgesetzt haben sich abteilungs- oder bereichsbezogene Schulungen, in denen Mitarbeiter mit nahezu gleichem Umgang mit personenbezogenen Daten teilnehmen. Möglich ist daher auch die Zusammenlegung von Abteilungen oder Bereichen.

Die Gestaltung des Schulungsplans ist in Abhängigkeit der zu schulenden Mitarbeiterinnen und Mitarbeiter zu erstellen. Da das Unternehmen eine dezentrale Struktur hatte, ist es in einigen Bereichen sinnvoll gewesen, die entsprechenden Schulungen durch die zuständigen Regionalleiter vor Ort durchführen zu lassen.

Im Internet werden verschiedene Formulare zum Erwerb angeboten. Diese sollen helfen, den Aufwand auf ein vertretbares Minimum zu reduzieren.

Dieses wiederum erfordert eine ausführliche Schulung der entsprechenden Bereichsleiter. Hierzu wurde seitens des externen Datenschutzbeauftragten ein Mitarbeiter entsandt, der in zwei Tagen à acht Stunden diese Personen schulen sollte.

763 *Reimann/e.V.,* Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung, 2. Aufl. 2018, 12.2 Unterweisungen, S. 134 und 135.

2.4 Datenschutz – und Compliance-Risiken

2.4.1 Begriffe

Zur besseren Erfassung des bzw. der Themen ist eine kurze Erläuterung über die Begrifflichkeiten der Unterpunkte, Compliance und Risiko erforderlich. Bei Recherchen zu diesem Thema wurde festgestellt, dass die Begriffe sehr gerne miteinander vermengt werden, ohne eine wirkliche Abgrenzung untereinander zu definieren.

2.4.1.1 Compliance

Gabler Wirtschaftslexikon definiert den Begriff Compliance wie folgt: engl. Begriff, ***sinngemäß*** **Einhaltung von Gesetzen, Regeln und Normen**. Ursprünglich auf die Bankwirtschaft und das Gesundheitsmanagement begrenzt, inzwischen breit eingesetzt, z.B. IT-Compliance, Global Compliance, Tax Compliance, Customs Compliance, **Datenschutz Compliance**, dass mithilfe von **C**ompliance **M**anagement **S**ystemen (**CMS**) und personifiziert durch den Compliance-Officer durchgeführt wird (u.a. im Rahmen des Risikomanagements).[764]

Compliance beschreibt die Gesamtheit der Maßnahmen eines Unternehmens zur Vermeidung von Gesetzesübertretungen und sonstigen Maßnahmen zur Vermeidung von Regelverstößen. Die Einführung der DS-GVO[765] bedeutet aus Compliance-Gesichtspunkten zunächst ein extrem gestiegenes Bußgeldrisiko, welches es bei den Gefährdungsanalysen zu berücksichtigen gilt. Diese Gefährdungsanalyse erfordert eine tiefgehende Auseinandersetzung mit den Anforderungen der DS-GVO. Effektive Compliance-Strukturen setzen (unter anderem) Kontrollen von Mitarbeitern und Geschäftspartnern voraus, die mit den Persönlichkeitsrechten der betroffenen Person in Einklang zu bringen sind. Präventive Compliance-Kontrollen dürfen gemäß Art. 88 Abs. 2 DS-GVO i.V.m. § 32 BDSG[766] als Zwecke der Durchführung des Beschäftigungsverhältnisses zu bewerten sein. Weiterhin können auch Betriebsvereinbarungen als eine Erlaubnisnorm für Compliance-Maßnahmen dienen.

764 *Gabler Wirtschaftslexikon,* Compliance, https://wirtschaftslexikon.gabler.de/definition/compliance-27721/version-333143.

765 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).

766 Bundesdatenschutzgesetz, BDSG - Bundesdatenschutzgesetz.

Allerdings müssen solche Betriebsvereinbarungen den Anforderungen der DS-GVO genügen. Interne Ermittlungen und Compliance-Maßnahmen zur Aufdeckung von Straftaten im Unternehmen müssen künftig über Art. 6 Abs. 1 lit. f DS-GVO gerechtfertigt werden. Hierfür müsste das Aufklärungsinteresse die Datenverarbeitung rechtfertigen.[767]

2.4.1.2 Risiko

Allgemein wird der Begriff „Risiko" wie folgt definiert: Kennzeichnung der Eventualität, dass mit einer (ggf. niedrigen, ggf. auch unbekannten) Wahrscheinlichkeit (ggf. hoher, ggf. in seinem Ausmaß unbekannter) Schaden bei einer (wirtschaftlichen) Entscheidung eintritt oder ein erwarteter Vorteil ausbleiben kann.[768]

Der Begriff des Risikos ist in der DS-GVO nicht definiert. Allerdings finden sich in **Erwägungsgrund 75**[769] und **Erwägungsgrund 94** Satz 2. Anknüpfungspunkte, aus denen die folgende Definition hergeleitet wird: Ein Risiko im Sinne der DS-GVO ist das Bestehen einer Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden darstellt oder zu einem Schaden natürlicher Personen führen kann.[770]

2.4.2 IT-Compliance

Angesichts der stetig zunehmenden Komplexität von Geschäftsprozessen in einem Unternehmen und der Abhängigkeit des Unternehmens vom Funktionieren der EDV ist die Steuerung eines Unternehmens ohne den Einsatz von Informationstechnologie (IT) nicht mehr vorstellbar. Corporate Governance und Compliance sind damit untrennbar mit IT-Compliance verbunden, also dem verantwortlichen Umgang mit allen Aspekten von IT. Der Begriff IT-Compliance reicht dabei von der Einhaltung von Datenschutz und der Sicherstellung von IT-Sicherheit über den rechtskonformen Umgang mit Lizenzen bis hin zur gesetzeskonformen E-Mail-Archivierung und Kontrolle der IT-Nutzung der Mitarbeiter.[771]

---

767 *Wybitul,* EU-Datenschutz-Grundverordnung im Unternehmen, 2016, S. 134 Compliance.
768 *Gabler Wirtschaftslexikon,* Definition Risiko, https://wirtschaftslexikon.gabler.de/definition/risiko-44896/version-268200.
769 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 75.
770 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, S. 577, Art. 24, Rn. 32.
771 *A. Becker,* Corporate Compliance Checklisten, S. 195, Rn. 1.

2.4.3 Datenschutz-Risikomanagement

Um als Verantwortlicher datenschutzkonform zu handeln und die Vorschriften des DS-GVO einzuhalten, ist eine angemessene Berücksichtigung der Risiken von zentraler Bedeutung. Der Begriff des Risikos kommt an verschiedenen Stellen in der DS-GVO vor (z.B. Art. 35, 36; Datenschutzfolgeabschätzung und Art. 33, 34; Datenschutzverletzungen) und sollte einheitlich interpretiert und angewandt werden. Der Risikobegriff ist in der Verordnung nicht definiert, wenngleich Beispiele für Risiken genannt werden (u. A. ErwGr. 75). Dabei muss zwischen unterschiedlichen Risikoarten differenziert werden (z.B. Datenschutzrisiken und Compliance-Risiken).[772]

Erwägungsgrund 75

Die Risiken für die Rechte und Freiheiten natürlicher Personen mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere können aus einer Verarbeitung personenbezogener Daten hervorgehen. Im Besonderen in Fällen:

- Wenn es zu physischen, materiellen oder immateriellen Schaden führen könnte,
- Weiterhin wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann,
- Insofern die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren,
- In Fällen in welchen personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende

772 *Sachs/Kranig/Gierschmann,* Datenschutz-Compliance nach der DS-GVO, 2017, S. 78, Punkt 6 Datenschutz-Risikomanagement.

Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden,

- Darüber hinaus, wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen,
- Wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder
- Wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.[773]

2.4.4 Risikobezug in der DS-GVO

Der Verantwortliche muss bei jeder Verarbeitung personenbezogener Daten die Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen, die mit der Verarbeitung personenbezogener Daten einhergehen und zu einem physischen, materiellen oder immateriellen-Schaden für den Betroffenen führen können (Art. 24)[774]. Die Einschätzung von Risiken ist ferner bei der Sicherheit von Verarbeitungen (Art. 32) sowie Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25) relevant. Kommt man bei der Einschätzung zu einem voraussichtlich „hohen Risiko", muss der Verantwortliche außerdem vor Aufnahme einer Verarbeitung eine Datenschutz-Folgeabschätzung durchführen (Art. 35 und 36). Der Verantwortliche muss insgesamt den Risiken entsprechend geeignete technische und organisatorische Maßnahmen umsetzen.[775]

Schließlich spielt der Risikobegriff auch bei der Handhabung von Datenschutzverletzungen eine wichtige Rolle. Denn von der Einstufung des Risikos (kein

773 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 75.

774 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 24 DSGVO.

775 *Sachs/Kranig/Gierschmann,* Datenschutz-Compliance nach der DS-GVO, 2017, S. 78, Abschnitt 6.1 Risikobezug in der DSGVO.

Risiko, Risiko oder hohes Risiko) hängt ab, welche Schritte er unternehmen muss. Bei einer Datenschutzverletzung mit einem möglichen Risiko für die Betroffenen muss er zunächst die Verletzung der Aufsichtsbehörde melden (Art. 33). Handelt es sich aber möglicherweise um ein „hohes Risiko“, hat der Verantwortliche außerdem die Betroffenen zu benachrichtigen (Art. 34).[776]

Nachfolgende Abbildung zeigt das Datenschutz-Risiko in den einzelnen Vorschriften auf:

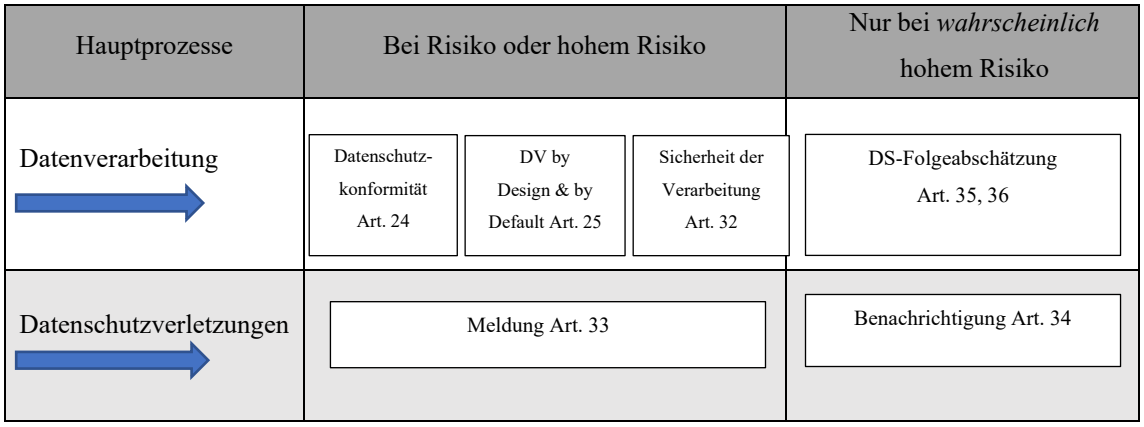

Abbildung 8: Der Begriff Risiko in einzelnen Vorschriften[777]

2.4.5 Risikobeurteilung

In ErwGr. 76 wird explizit eine Risikobeurteilung anhand einer objektiven – d.h. einer nachvollziehbaren – Risikobewertung gefordert, durch die eine Risikoklassifikation einer Datenverarbeitung in ein Risiko oder ein hohes Risiko möglich ist. [778] Der ErwGr. 77 zeigt erforderliche Schritte im Umgang mit Risiken auf.[779]

776 *Sachs/Kranig/Gierschmann,* Datenschutz-Compliance nach der DS-GVO, 2017, S. 78, Abschnitt 6.1 Risikobezug in der DSGVO.

777 *Sachs/Kranig/Gierschmann,* Datenschutz-Compliance nach der DS-GVO, 2017, Abbildung 24, S. 79, Der Begriff Risiko in den einzelnen Vorschriften.

778 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 76.

779 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Entspricht in etwa der Formulierung in Erwägungsgrund 90, d.h., die Risikobewertung nach Art. 24 und Art. 35 DSGVO.

- Ermittlung des mit der Verarbeitung verbunden Risikos: Abschätzung des Risikos in Bezug auf Ursache, Art, Eintrittswahrscheinlichkeit und Schwere und Festlegung von Verfahren für dessen Eindämmung
- Durchführung geeigneter Maßnahmen
- Nachweis der Einhaltung[780]

Erwägungsgrund 76

Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.[781]

Erwägungsgrund 77

Anleitungen, wie der Verantwortliche oder Auftragsverarbeiter geeignete Maßnahmen durchzuführen hat und wie die Einhaltung der Anforderungen nachzuweisen ist, insbesondere was die Ermittlung des mit der Verarbeitung verbundenen Risikos, dessen Abschätzung in Bezug auf Ursache, Art, Eintrittswahrscheinlichkeit und Schwere und die Festlegung bewährter Verfahren für dessen Eindämmung betrifft, könnten insbesondere in Form von genehmigten Verhaltensregeln, genehmigten Zertifizierungsverfahren, Leitlinien des Ausschusses oder Hinweisen eines Datenschutzbeauftragten gegeben werden. Der Ausschuss kann ferner Leitlinien für Verarbeitungsvorgänge ausgeben, bei denen davon auszugehen ist, dass sie kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, und angeben, welche Abhilfemaßnahmen in diesen Fällen ausreichend sein können.[782]

780 *Sachs/Kranig/Gierschmann,* Datenschutz-Compliance nach der DS-GVO, 2017, S. 80, Risikobeurteilung.

781 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 77.

782 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 76.

Nachfolgende Grafik zeigt eine Möglichkeit auf, Risiken anhand eines Punktesystems zu beurteilen. Dieses ist individuell anpassbar und stellt lediglich eine Möglichkeit der Beurteilung dar.

Risikobeurteilung

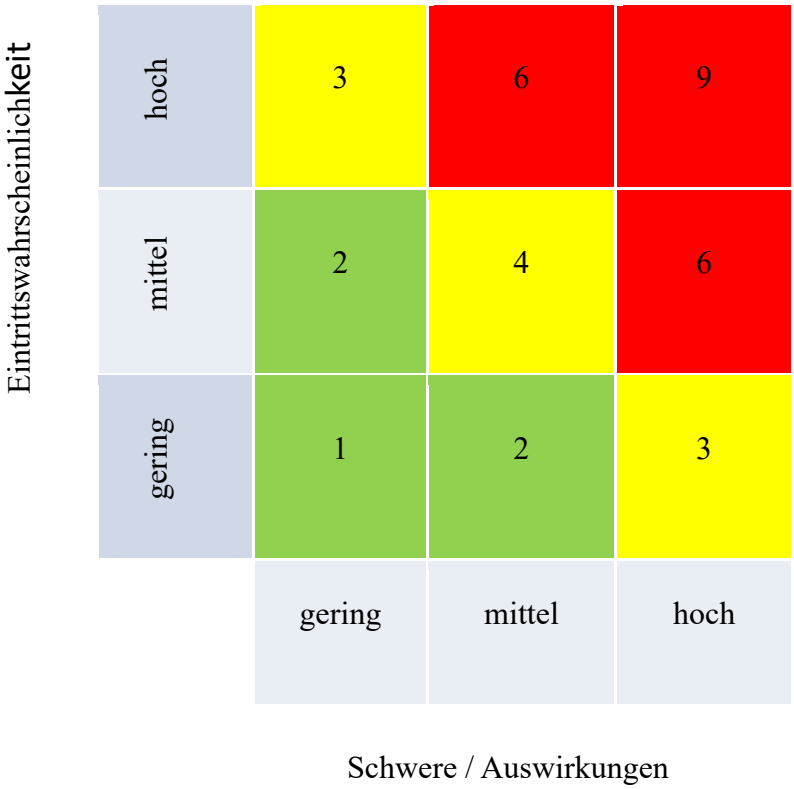

Abbildung 9: Risikobeurteilung

Anhand der Ergebnisse einer Risikobeurteilung ist eine Eintrittswahrscheinlichkeit für ein mögliches Risiko im Bereich der DS-GVO bestimmbar. Aufgrund dieser Tatsache ist eine Umsetzung bezüglich der Verhinderung möglicher Risiken möglich.

2.4.6 Risikomanagementprozess

Der „Risikomanagementprozess“ (risk management process) ist schließlich die systematische Anwendung von Richtlinien, Verfahren und Praktiken aus allen risikoorientierten Maßnahmen, wie z.B. Identifikation, Analyse, Bewertung und

Behandlung von Risiken sowie die damit verbundene Überwachung und Überprüfung einschließlich Kommunikation und Konsultation.[783]

Nach ISO 31000[784] besteht der Risikomanagementprozess aus nachfolgenden Schritten:

- **Festlegung des Kontextes**: Festlegung der externen und internen Parameter, die beim Risikomanagement berücksichtigt werden müssen; Bestimmung des Umfangs und der Risikokriterien für die Risikomanagement-Richtlinie
- **Risikobeurteilung**: Prozess der Risikoidentifikation, -analyse und -bewertung
- **Risikobehandlung**: Prozess zur Modifikation der Risiken (z.B. Risiko tragen, reduzieren, übertragen oder vermeiden)
- **Risikoüberwachung und -überprüfung**: Fortlaufende Steuerung und Kontrolle der Durchführung der Risikomaßnahmen, des Risikomanagementprozesses sowie des Risikomanagementsystems hinsichtlich Angemessenheit und Wirksamkeit
- **Risikokommunikation und -konsultation**: Kontinuierlicher und iterativer Prozess, um Informationen zu erheben, zu teilen und um die Stakeholder am Dialog bzgl. des Managements von Risiken zu beteiligen.[785]

783 *Sachs/Kranig/Gierschmann,* Datenschutz-Compliance nach der DS-GVO, 2017, S. 92, Abschnitt 6.2.2.3 Abs. 1.
784 DIN ISO 31000:2018-10 10.2018.
785 *Sachs/Kranig/Gierschmann,* Datenschutz-Compliance nach der DS-GVO, 2017, S. 92, Abschnitt 6.2.2.3 Abs. 2.

Der Risikomanagementprozess lässt sich grafisch wie folgt darstellen:

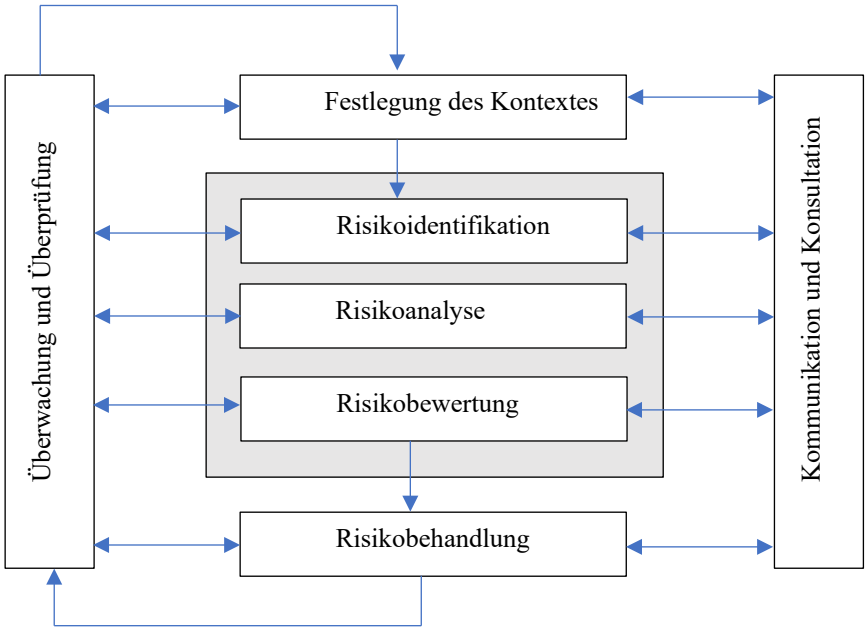

Abbildung 10: Risikomanagementprozess nach ISO 31000:2009

Abbildung 10 stellt diesen idealtypischen Risikomanagement-Regelkreis gemäß dem internationalen Risikomanagement-Standard ISO 31000[786] dar. Diese Phasen werden nachfolgend skizziert.[787]

Das Risikomanagement beginnt damit, die Rahmenbedingungen für das Risikomanagement zu definieren (**Festlegung des Kontextes**). In dieser auch als „Risikomanagement-Strategie" bezeichneten Phase werden zum einen die Einbindung des Risikomanagements in der Aufbauorganisation festgelegt, zum anderen aber auch Schwellenwerte für Risiken spezifiziert. Neben einer Definition des externen Zusammenhangs (soziale, kulturelle, politische, rechtliche, regulatorische, finanzielle, technologische, wirtschaftliche, natürliche und wettbewerbsspezifische Gegebenheiten internationaler, nationaler, regionaler oder lokaler Art) liegt ein weiterer Schwerpunkt bei der Erstellung des internen Zusammenhangs (Governance-Struktur, organisatorischer

786 DIN ISO 31000:2018-10 10.2018.
787 *Romeike,* Risikomanagement, 2018, S. 36, Abschnitt 2.2 Regelkreis der Risikomanagements, Abs. 2.

Aufbau, Rollen und Verantwortlichkeiten, Strategien, Ressourcen, Informationssysteme etc.).[788]

Um Risiken wirkungsvoll handhaben zu können, müssen diese bekannt sein. Die **Risikoidentifikation** dient dazu, Risiken aufzuspüren. Hierbei sollten Risikoquellen, betroffene Bereiche, Ereignisse und Entwicklungen im Zeitverlauf berücksichtigt werden. Diese Phase führt damit zu einem qualitativen Ergebnis.[789]

In der Prozessphase der **Risikoanalyse** soll ein besseres Verständnis für ein Risiko generiert werden. Die Risikoanalyse fließt in die Risikobewertung und in Entscheidungen darüber ein, welche Strategien und Methoden der Risikobewältigung für sie am besten geeignet sind. Die Risikoanalyse betrachtet die Ursachen und Quellen der Risiken, ihre positiven und negativen Auswirkungen sowie die Häufigkeit bzw. Wahrscheinlichkeit ihres Eintretens. Das Risiko wird durch eine Bestimmung der potenziellen Auswirkungen analysiert. Die Risikoanalyse kann je nach Risiko, Zweck der Risikoanalyse und den verfügbaren Informationen, Daten und Ressourcen mit unterschiedlicher Untersuchungstiefe durchgeführt werden.

Da die DS-GVO einen risikobasierten Datenschutzansatz verfolgt, hängt der Umfang der Datenschutzpflichten des Unternehmens vom Risikopotenzial der Verarbeitungstätigkeiten bzgl. des Schutzes der Rechte und Freiheiten der betroffenen Personen ab. Zudem wird die Umsetzung der neuen Datenschutzstandards einen hohen Aufwand erfordern, sodass die Pflichten nicht alle zeitgleich umgesetzt werden können. Deshalb sollten Unternehmen prüfen, welche Vorgänge am risikoreichsten sind und deshalb als erstes in Einklang mit den Vorgaben der DS-GVO gebracht werden müssen. Die Risiko-Analyse sollte sich darauf konzentrieren, diejenigen Verarbeitungsvorgänge zu identifizieren, die mit dem größten Risiko für das Geschäft des Unternehmens und die Rechte der betroffenen Personen verbunden sind und/oder die am wahrscheinlichsten zu hohen Bußgeldern im Falle von Datenschutzverletzungen führen werden. Die Anstrengungen zur Einhaltung eines angemessenen Datenschutzniveaus müssen für risikoreiche Verarbeitungsvorgänge besonders verstärkt werden, indem diese zuerst

788 *Romeike,* Risikomanagement, 2018, S. 36, Abschnitt 2.2 Regelkreis der Risikomanagements, Abs. 3.

789 *Romeike,* Risikomanagement, 2018, S. 36, Abschnitt 2.2 Regelkreis der Risikomanagements, Abs. 4.

behandelt werden sollten. Die zweite Phase der Risikoanalyse wird mit der Erstellung eines groben strategischen Projektplans zur Umsetzung der neuen Datenschutzstandards geschlossen, der sich an der identifizierten Datenschutz-„Lücke“ unter Berücksichtigung des Risikopotenzials der verschiedenen Verarbeitungsvorgänge ausrichtet.[790]

In der **Risikobewertung** werden, die bisher erarbeiteten, qualitativen Ergebnisse quantifiziert. Es folgt eine Bewertung der Risiken durch potenzielle Schäden oder Schadensszenarien und den damit verknüpften Häufigkeiten bzw. Eintrittswahrscheinlichkeiten. Die im Rahmen der Risikoabschätzung erarbeiteten Informationen, vor allem die bewerteten, aggregierten und priorisierten Risiken, dienen anschließend als Grundlage für die Risikosteuerung.[791]

Die beschriebenen Phasen des Risikomanagement-Regelkreises werden parallel überwacht. Durch diese **Risikoüberwachung** wird sichergestellt, dass die Risikomanagement-Phasen korrekt durchgeführt werden, dass die Maßnahmen zur Risikosteuerung richtig umgesetzt werden und die beabsichtigte Wirkung entfalten.[792]

2.4.7 Techniken zur Risikobeurteilung

Die wichtigste Zielsetzung der Risikobeurteilung ist, die Risiken zu verstehen und potenzielle Auswirkungen einschätzen zu können. Dies setzt die Risikoidentifikation in Bezug auf die Ziele voraus (z.B. Risiken für das Unternehmen resultierend aus einem bestimmten Geschäftsprozess). Hierbei spielen auch Ursache und Wirkung eines Risikos eine Rolle.[793]

In der ISO 31000[794] werden vor allem die Methode des Risikomanagements und der Risikomanagementprozess behandelt. Die ISO 31010[795] befasst sich mit der praktischen Anwendung der Risikobeurteilung (risk assessment) und stellt Techniken zur Verfügung.

790 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, S. 323, Abschnitt 10.2, Schritt 2: Risikoanalyse.
791 *Romeike,* Risikomanagement, 2018, S. 37, Regelkreis der Risikomanagements, Abs. 1.
792 *Romeike,* Risikomanagement, 2018, S. 37, Regelkreis der Risikomanagements, Abs. 2.
793 *Sachs/Kranig/Gierschmann,* Datenschutz-Compliance nach der DS-GVO, 2017, S. 93, Abschnitt 6.2.2.4 Techniken zur Risikobeurteilung, Abs. 1.
794 DIN ISO 31000:2018-10 10.2018.
795 Risk Management - Risk assessment techniques, ISO/IEC 31010:2009.

Sie können einem Verantwortlichen als Orientierung für ein Risikomanagement dienen.[796]

Die Auswahl, der über 30 Techniken zur Risikobeurteilung der ISO 31010[797] ist, allgemeiner Natur, die sich in folgende Methodengruppen zusammenfassen lässt:

- Nachschlagemethoden, wie z.B. Checklisten
- Unterstützende Methoden, wie z.B. Brainstorming
- Szenario-Analysen
- Maßnahmen-Analysen
- Wirtschaftlichkeitsanalysen, wie z.B. Kosten-Nutzen-Analyse oder Gesamtbetriebskosten (Total Cost of Ownership)[798]

2.4.8 Risikobasierte Ansatz, (Art. 24 Abs. 1 Satz 1 DS-GVO)

Entsprechend dem in Art. 24 Abs. 1 Satz 1 DS-GVO verankerten risikobasierten Ansatz sind die technischen und organisatorischen Maßnahmen in Abhängigkeit des von einer Verarbeitung ausgehenden Risikos für die Rechte und Freiheiten natürlicher Personen zu treffen. Dieser risikobasierte Ansatz ist ein prägendes Element der DS-GVO, das an vielen Stellen der DS-GVO berücksichtigt wurde, z.B. beim Datenschutz durch Technikgestaltung gem. Art. 25 Abs. 1 DS-GVO[799], bei der Sicherheit der Verarbeitung gem. Art. 32 Abs. 1 und 2 DS-GVO, bei der Benachrichtigungspflicht im Fall von Datenschutzverletzungen gem. Art. 34 DS-GVO und bei der Datenschutz Folgenabschätzung gem. Art. 35 Abs. 1 DS-GVO.[800]

Die DS-GVO verfolgt einen risikobasierten Ansatz im Hinblick darauf, welche technischen und organisatorischen Datenschutzmaßnahmen in einer spezifischen Verarbeitungssituation angemessen sind. Das erforderliche Datenschutzniveau ist im

---

796 *Sachs/Kranig/Gierschmann,* Datenschutz-Compliance nach der DS-GVO, 2017, S. 93, Abschnitt 6.2.2.4 Techniken zur Risikobeurteilung, Abs. 2.

797 Risk Management - Risk assessment techniques, ISO/IEC 31010:2009.

798 *Sachs/Kranig/Gierschmann,* Datenschutz-Compliance nach der DS-GVO, 2017, S. 93, Abschnitt 6.2.2.4 Techniken zur Risikobeurteilung, Abs. 3.

799 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 25 DSGVO.

800 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, S. 576, Art. 24 DSGVO, Rn. 29 Risikobasierter Ansatz.

Einzelfall auf Grundlage einer objektiven Risikobewertung zu bestimmen.[801] Die Bewertung sollte hauptsächlich auf potenzielle Risiken für betroffene Personen Bezug nehmen, wobei auch die Risiken für bzw. durch Dritte sowie Verantwortliche/ Auftragsverarbeiter zu berücksichtigen sind.[802]

2.4.8.1 Risiken für betroffene Personen

Da Datenverarbeitungen in Grundrechte der betroffenen Personen eingreifen, müssen die legitimen Interessen an deren Durchführung mit dem Interesse an einem effektiven Datenschutz in Einklang gebracht werden. Dies betrifft insbesondere solche Risiken, die durch die unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw. unbefugten Zugang zu personenbezogenen Daten entstehen, Art. 32 Abs. 2 DS-GVO.

Ein erhöhtes Risiko besteht, wenn:[803]

- Die Wahrscheinlichkeit des Eintretens von Diskriminierungen, Identitätsdiebstahl oder –betrug, einem finanziellen Verlust, einer Rufschädigung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen besteht;
- Betroffene Personen um ihre Rechte und Freiheiten gebracht werden können oder an der Ausübung einer Kontrolle über ihre personenbezogenen Daten gehindert werden könnten;
- Besondere Kategorien personenbezogener Daten (vgl. dazu Art. 9 Abs. 1 DS-GVO) betroffen sind;
- Persönliche Aspekte, bspw. die Vorlieben der betroffenen Person, ausgewertet werden;
- Personenbezogene Daten von Kindern oder anderen schutzbedürftigen Personen verarbeitet werden;

801 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 76.

802 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, S. 50, Abschnitt 3.3.3 Abs. 1.

803 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 75.

- Eine große Menge personenbezogener Daten oder eine große Anzahl betroffener Personen betroffen ist.[804]

2.4.8.2 Risiken durch Dritte

Im Rahmen der Interessenabwägung müssen auch identifizierbare Risiken für die Rechte und Freiheiten der betroffenen Personen durch Dritte berücksichtigt werden. Dies betrifft u. a. Situationen, in denen sich staatliche Stellen über eine Intervention Zugang zu den Daten verschaffen können (z. B. in Bezug auf Telekommunikationsdaten, Fluggastdaten, …).[805]

2.4.8.3 Risiken für Verantwortliche und Auftragsverarbeiter

Zudem sind auch die drohenden Risiken für Verantwortliche und Auftragsverarbeiter zu berücksichtigen. Relevante Faktoren für die Entwicklung angemessener Maßnahmen sind die Kosten der Einbindung von Schutzmaßnahmen sowie Art, Umfang, Kontext und Zweck(e) der Datenverarbeitung, Art. 32 Abs. 1 DS-GVO. Die Risiken für Verantwortliche und Auftragsverarbeiter sind z. B.:

- Rechtliche Risiken, die sich aus seiner Verletzung von Datenschutzpflichten ergeben (z. B. Bußgelder, andere Sanktionen, …);
- Finanzielle Risiken (z. B. Schadensersatzforderungen, Kosten für die Verbesserung des Datenschutz-Managementsystems, …);
- Geschäftliche Risiken (z. B. Risiken für den Ruf des Unternehmens, das Nichterreichen von Geschäftszielen, Überbelastung des Managements, …).

Obwohl die Interessen von Verantwortlichen und Auftragsverarbeitern eine Rolle für die Risikobewertung spielen, sind sie nicht geeignet, eine generelle Herabsetzung des von der DS-GVO vorgeschriebenen Datenschutzniveaus zu rechtfertigen.[806]

804 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, S. 50 und 51, Abschnitt 3.3.3, Risiken durch Dritte.

805 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, S. 50, Abschnitt 3.3.3, Risiken für betroffene Personen.

806 *Voigt/dem Bussche,* EU-Datenschutz-Grundverordnung (DSGVO), 2018, S. 51, Risiken für Verantwortliche und Auftragsverarbeiter.

2.4.8.4 Contra risikobasierter Ansatz

Bereits während der Verhandlungen zur DS-GVO wurde der risikobasierte Ansatz kritisiert. Hier bediente man sich z.T. polemischer Behauptungen. So wurde der risikobasierte Ansatz als trojanisches Pferd der Datenschutzreform bezeichnet.[807] Auf der sachlichen Ebene wurde die Befürchtung geäußert, dass durch den risikobasierten Ansatz die Pflichten der datenverarbeitenden Unternehmen sowie die Rechte der Betroffenen reduziert werden sollten.[808] Ein beachtliches Argument, das gegen den risikobasierten Ansatz vorgebracht wurde, ist, dass eine Risikoabschätzung durch den Verantwortlichen regelmäßig an sämtlichen Betroffenen eines bestimmten Verarbeitungsvorgangs im Kollektiv vorgenommen werden dürfte und damit das individuelle Risiko eines Betroffenen außer Acht gelassen werde. Dieses Argument ist aber nur teilweise tragfähig, da i.R.d. Beurteilung einer Datenschutzverletzung auch das Risiko für die betroffene Person zu prüfen ist. Damit wird deutlich, dass die Risikobewertung nach der DS-GVO unterschiedliche Schwerpunkte hat.[809] Eine weitere beachtliche Position gegen den risikobasierten Ansatz geht davon aus, dass sich die Asymmetrie zwischen den Verantwortlichen und den Betroffenen vergrößere, wenn die das Risiko begründende Stelle zugleich über die Tragbarkeit dieses Risikos entscheide. Auch dieses Argument vermag jedoch nur teilweise zu überzeugen, da isoliert auf den Schutzzweck der Informationsasymmetrie abgestellt wird.[810]

---

807 *Bergmann, Benjamin*, EU-Ministerrat reitet auf Trojanischen Pferden Richtung Datenschutzreform 11.3.2013, https://netzpolitik.org/2013/innen-und-justizminister-reiten-auf-trojanischen-pferden-richtung-datenschutzreform/.

808 *Albrecht*, Albrecht, PM v. 7.3.2013, abrufbar unter: https://www.gruen-digital.de/2013/03/eu-datenschutz-ministerrat-muss-beim-datenschutz-liefern/; vzbv, PM v. 25.11.2014, abrufbar unter: https://www.vzbv.de/pressemitteilung/eu-datenschutzverordnung-weichen-stellen-fuer-mehr-datenschutz-0. 07.03.2013.

809 *Datenschutzgruppe 29,* Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, WP 250 rev.01: Guidlines on Personal Data breach notification und der Regulation 2016/679, S. 23.

810 *Schröder, Markus*, Der risikobasierte Ansatz in der DSGVO, Risiko oder Chance für den Datenschutz, in ZD - Zeitschrift für Datenschutz, 503.

2.4.8.5 Pro risikobasierter Ansatz

Der begrenzte risikobasierte Ansatz, der letztlich auch Eingang in die DS-GVO gefunden hat, geht davon aus, dass die grundlegenden datenschutzrechtlichen Prinzipien durch diesen Ansatz nicht ersetzt werden sollen.[811] Es gehe vielmehr um eine Skalierung der zu ergreifenden Maßnahmen auf Basis eines Risikomanagements.[812] Dieser Ansatz wurde in Teilen der Literatur allerdings nicht als große Neuerung, sondern eher als Feststellung einer Selbstverständlichkeit angesehen: „We have always managed risks in data protection law",[813] „Understanding data protection as risk regulation"[814] oder „Why the GDPR risk-based approach is about compliance risk, and why it's not a bad thing".[815] Auf der anderen Seite wurde aber auch zu bedenken gegeben, dass man nicht beides habe könne: einen risiko-basierten Ansatz und ein Festhalten an den bisherigen datenschutzrechtlichen Grundprinzipien.[816] Daher wurde folgerichtig auch die Frage aufgeworfen, ob Art. 24 Abs. 1 DS-GVO auch für die Grundsätze der Datenverarbeitung, für die Rechtsgrundlagen und für die Betroffenenrechte gelte. De lege lata sprechen aber rechtssystematische Erwägungen eher gegen diese Auffassung, da Art. 24 Abs. 1 DS-GVO nicht „vor die Klammer gezogen" als Grundsatz in Art. 5 DS-GVO formuliert wurde.[817]

811 CIPL (o. Fußn. 4), S. 4; Kuner/Cate/Millard/Svantesson/Lynskey, IDPL 2015, 95, 96.
812 *Drackert, Thoma* (Hrsg.), Thoma, ZD 2013, 578, 580 f; Drackert (o. Fußn. 34), S. 280 ff. (zit. als *Bearbeiter* in Drackert).
813 *Gellert* (Hrsg.), EDPL 2016, 481 (zit. als *Bearbeiter* in Gellert).
814 *Gellert* (Hrsg.), Journal of Internet Law 2015, 3 (zit. als *Bearbeiter* in Gellert).
815 *Gellert* (Hrsg.), IRIS 2017 Tagungsband, S. 527 (zit. als *Bearbeiter* in Gellert).
816 *EU-Data Protection Law* (Hrsg.), The risk revolution in EU data protection law, S. 21 f., abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3000382. (zit. als *Bearbeiter* in EU-Data Protection Law).
817 *Schröder, Markus*, Der risikobasierte Ansatz in der DSGVO, Risiko oder Chance für den Datenschutz, in ZD - Zeitschrift für Datenschutz, 503.

2.5 Verfahrensverzeichnis (Art. 30 DS-GVO)

2.5.1 Überblick

Die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten ist ein Teil der aus dem Accountability-Prinzip nach Art. 5 Abs. 2 i.V.m. Art. 24 resultierenden Pflicht, die Einhaltung der DS-GVO nachweisen zu können. Dazu dient nach Erwägungsgrund 82 das Verzeichnis von Verarbeitungstätigkeiten in der Zuständigkeit des Verantwortlichen oder Auftragsverarbeiters. Insbesondere soll es der Zusammenarbeit mit den Aufsichtsbehörden dienen: Nach **Erwägungsgrund 82** soll die Pflicht zur Vorlage des Verzeichnisses gegenüber den Aufsichtsbehörden ermöglichen, dass diese die betreffenden Verarbeitungsvorgänge anhand des Verzeichnisses kontrollieren können.[818]

Erwägungsgrund 82

Zum Nachweis der Einhaltung dieser Verordnung sollte der **Verantwortliche** oder der **Auftragsverarbeiter** ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser **auf Anfrage** das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.[819]

2.5.2 Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO)

Die im Anhang befindliche Tabelle ist eine Vorlage für die Erfüllung der sich aus Art. 30 Abs. 1 DS-GVO ergebenden Pflicht des Verantwortlichen und ggf. seines Vertreters i. S. d. Art. 27 DS-GVO zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten. Die Erläuterungen zum Muster gehen davon aus, dass insgesamt nur ein Verzeichnis geführt wird und darin alle in den §§ 1 und 2 genannten Angaben enthalten sind. Der Begriff „Verfahrensverzeichnis“ war dem BDSG a. F. fremd, konnte sich in der Praxis jedoch durchgesetzt und wird mutmaßlich auch zukünftig für das Verzeichnis von Verarbeitungstätigkeiten verwendet werden. Die früher gebräuchliche Unterscheidung zwischen dem „internen Verfahrensverzeichnis“ und dem „Jedermann-Verzeichnis“

818 *Bäcker,* Datenschutz-Grundverordnung, S. 583, Rn. 1, Art. 30 Abs. 1 DSGVO.
819 Amtsblatt der Europäischen Union 04.05.2016 (Erwägungsgrund 82 DSGVO).

i. S. d. § 4 g Abs. 2 S. 2 BDSG a. F. hat sich mit der DS-GVO erledigt, da es keine Verpflichtung mehr gibt, das Verfahrensverzeichnis ganz oder teilweise jedermann zugänglich zu machen. Mit Art. 30 Abs. 1 DS-GVO ist nur das interne Verfahrensverzeichnis übriggeblieben, welches der Aufsichtsbehörde gem. Art. 30 Abs. 4 DS-GVO nur auf Anfrage zur Verfügung zu stellen ist.[820]

2.5.3 Form und Bereitstellung (Art. 30 Abs. 3 DS-GVO)

Nach Art. 30 Abs. 3 DS-GVO ist die Dokumentation schriftlich zu führen, wobei bei Art. 30 Abs. 3 DS-GVO gleichzeitig klarstellt wird, dass die elektronische Form genügt.[821]

Es kann also explizit in einem elektronischen Format geführt werden. Dies ist nicht an die Form des deutschen Rechts i.S.d. § 126a BGB[822] gebunden.[823] Allerdings verpflichtet Art. 30 Abs. 4 den Verantwortlichen, das Verzeichnis der Aufsichtsbehörde auf Anfrage „zur Verfügung zu stellen". Daher muss ein elektronisch geführtes Verzeichnis exportierbar sein. Damit ist eine einfache Zusammenstellung von internen Hyperlinks nicht tauglich, wohl aber ein Dokument, das nach Anfrage der Aufsichtsbehörde aus Hyperlinks auf interne Dokumente und Informationen zusammengestellt wird.[824]

2.5.4 Ausnahmen (Art. 30 Abs. 5)

Die Dokumentation soll zur Vermeidung von Bürokratie und Kosten nicht für kleine und mittelständische Unternehmen gelten, weshalb in Art. 30 Abs. 5 DS-GVO eine Ausnahmeregelung vorgesehen ist. Die Ausnahmeregelung wird jedoch aufgrund ihrer inhaltlichen Anforderungen und der Bedeutung des Verzeichnisses von

820 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, S. 156, Art. 30 DSGVO.
821 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 30 Abs. 3 DSGVO in Verbindung mit Erwägungsgrund 82
822 *Palandt/Bassenge,* Bürgerliches Gesetzbuch, 74. Aufl. 2015, S. 112, § 126a BGB (Buch 1. Abschnitt 3.).
823 *Bäcker,* Datenschutz-Grundverordnung, S. 593, Rn. 32, Art. 30 Abs. 3 DSGVO.
824 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 37760 von 87533 Abs. 3, Rn. 80 DSGVO.

Verarbeitungstätigkeiten für eine Datenschutz-Folgenabschätzung kaum praktische Bedeutung erlangen.[825]

Art. 30 Abs. 5 normiert Ausnahmen von der Verzeichnisführungspflicht, die nach EG 13 für Kleinstunternehmen gelten sollen. Die Vorschrift besagt, dass kleine Unternehmen mit weniger als 250 Mitarbeiter[826] von der Pflicht befreit sind, wenn nicht eine der Gegenausnahmen eingreift.[827]

Von der Pflicht zum Führen eines Verzeichnisses der Verarbeitungstätigkeiten ausgenommen sind, „Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 einschließt, (vgl. Art. 30 Abs. 5 DS-GVO).[828]

Nachfolgende Tabelle zeigt die Definition der Europäischen Kommission in Bezug auf **KMU** (**k**leine und **m**ittlere **U**nternehmen).[829]

Unternehmensgröße	Zahl der Beschäftigten	*und*	Umsatz in € pro Jahr	*oder*	Bilanzsumme in € pro Jahr
kleinst	bis 9		bis 2 Mio.		bis 2 Mio.
klein	bis 49		bis 10 Mio.		bis 10 Mio.
mittel	bis 249		bis 50 Mio.		bis 43 Mio.

Abbildung 11: Definition KMU

825 *Rüpke/K. Lewinski/Eckhardt,* Datenschutzrecht, 2018, S. 249, Rn. 30, § 17. Verzeichnis von Verarbeitungstätigkeiten (2. Teil).
826 *T. Becker et al.,* DSGVO/BDSG, Plath in Plath Art. 30, Rn. 4 DSGVO.
827 *Bäcker,* Datenschutz-Grundverordnung, S. 593, Rn. 34, Art. 30 Abs. 5 DSGVO (Ausnahmen).
828 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, S. 157 Abs. 2.
829 *Europäische Union*, EMPFEHLUNG DER KOMMISSION vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (Bekannt gegeben unter Aktenzeichen K(2003) 1422) (2003/361/EG), L 124/36, Artikel 2, in Amtsblatt der Europäischen Union.

2.6 Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)

Die Datenschutz-Folgeabschätzung löst die in Art. 20 DSRL[830] geregelte Vorabprüfung ab, die für Verarbeitung mit spezifischen Risiken für die Rechte und Freiheiten der natürlichen Person verbindlich vorgesehen ist.[831]

Art. 35[832] führt das Konzept der Datenschutz-Folgenabschätzung (auf Englisch „Data **P**rotection **I**mpact **A**ssessment" oder kurz „**PIA**2 genannt) in das europäische Datenschutzrecht ein. Die Vorschrift greift die in Art. 20 DSRL[833] geregelte (und in § 4 Abs. 5 BDSG konkretisierte) Vorabkontrolle auf und entwickelt diese zu einer in der Unternehmenspraxis deutlich umfangreicheren Compliance-Anforderung weiter. Das Konzept basiert auf dem Grundsatz des risikobasierten Datenschutzes und verlangt von dem Verantwortlichen eine eigenverantwortliche und detaillierte Risikoanalyse der eigenen Datenverarbeitung. Die Datenschutz-Folgeabschätzung stellt damit eine besonders praxisrelevante Ausprägung des Grundsatzes der gesteigerten Eigenverantwortlichkeit der Unternehmen (auch „Accountability" genannt) dar, eines der grundlegenden Prinzipien der gesamten DS-GVO.[834]

Der für die Verarbeitung Verantwortliche muss einerseits jede relevante Datenverarbeitung dahingehend bewerten, ob diese mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der betroffenen Person behaftet ist. Andererseits enthält die DS-GVO keine konkrete Definition, mit deren Hilfe der Verantwortliche zu einer verlässlichen Einschätzung in der Lage wäre, ob das Risiko dermaßen hoch ist, dass es als Auslöser einer Datenschutz-Folgenabschätzung betrachtet werden muss. Die Einschätzung eines Risikos ohne objektive Leitlinien birgt die Gefahr, dass die Wertung

---

830 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates.

831 *Bäcker,* Datenschutz-Grundverordnung, S. 631, Art. 35, Hintergrund und Entstehungsgeschichte, Rn. 2.

832 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 35 DSGVO.

833 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, Art. 20 DSRL.

834 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, S. 618, Art. 35 DSGVO, Rn. 1.

der Risikolage einen subjektiven Einschlag erhält und in der Praxis zu erheblichen Unsicherheiten führen kann.[835]

Grundlage der Datenschutz-Folgeabschätzung ist somit Art. 24 Abs. 1 Satz 1 DS-GVO i.V.m. Art. 5 Abs. 2 DS-GVO. Bei ihr handelt es sich als zunächst um eine konkrete organisatorische Maßnahme, um sicherzustellen und den Nachweis dafür zu erbringen, dass die Verarbeitung im Einklang mit der DS-GVO erfolgt („Accountability“).[836]

Als Baustein des risikobasierten Konzepts zielt Art. 35 darauf ab, das normative Erwartungsniveau an Datenschutzmaßnahmen mit dem Risikoniveau zu synchronisieren, das der Verarbeitungsprozess auslöst – vor allem bei besonders persönlichkeitssensiblen Arten der Datenverarbeitung.[837]

Nachfolgende Grafik zeigt die Grundsätze der Datenschutz-Folgenabschätzung auf:

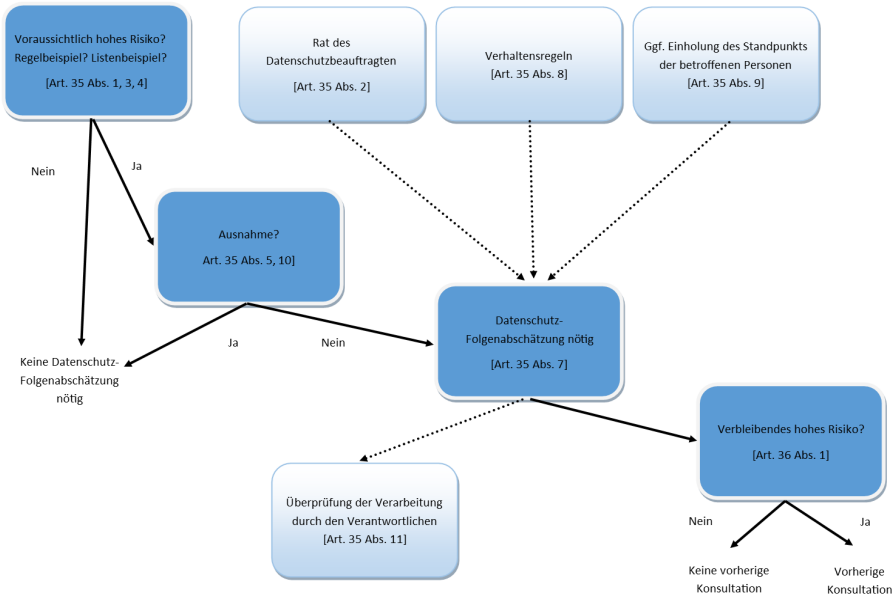

Abbildung 12: Prozess nach Art. 29-Datenschutzgruppe[838]

835 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Pos. 42308 von 87533, Rn. 2.

836 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, S. 775, Art. 35 DSGVO, Grundlagen und Zweck, Rn. 1 Abs. 2.

837 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, S. 500, Rn. 7, Sinn und Zweck der Vorschrift, Art. 35 DSGVO.

838 17/ EN WP 248 rev. 01: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk“ for the purposes of Regulation 2016/ 679, S. 9.

2.6.1 Durchführungspflicht, (Art. 35 Abs. 1 Satz 1 DS-GVO)

Aus Art. 35 Abs. 1 S. 1 ergeben sich jedoch mehrere **Anhaltspunkte**, welches zu erwartende Risiko als Auslöser einer Datenschutz-Folgenabschätzung in Frage kommt. So soll die Verwendung **neuer Technologien** das Risiko soweit erhöhen können, dass das Risiko die **Relevanzschwelle** einer Datenschutz-Folgenabschätzung zu überschreiten vermag. Die bestehende Unsicherheit hinsichtlich des Bestehens eines hohen Risikos wird jedoch durch die Bezugnahme auf Technologien oder neue Technologien nicht eliminiert, da beide Begriffe zwar in der DS-GVO erwähnt, aber dort weder näher beschrieben noch definiert werden.[839]

Art. 35 enthält keine Vorgaben zur praktischen Umsetzung der Verpflichtungen. Insbesondere aus den Vorschriften zum Mindestinhalt einer Datenschutz-Folgenabschätzung in Abs. 7 lassen sich aber wichtige Grundsätze ableiten.[840]

Gem. Art. 35 Abs. 1 S. 1[841] ist im Grundsatz eine Datenschutz-Folgenabschätzung vorzunehmen, wenn eine Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.[842]

Nicht ganz einleuchtend ist, weshalb Abs. 1 S. 1[843] von den Rechten und Freiheiten natürlicher Personen spricht, die DS-GVO jedoch an anderer Stelle, beispielsweise in Abs. 7 lit. c, den Begriff der „Rechte und Freiheiten der betroffenen Personen“ gemäß Art. 4 Nr. 1 verwendet.[844]

---

839 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Art. 35 Abs. 1 Satz 1, Heidelberger Kommentar, Position 42308 von 87533, Rn. 3.

840 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, S. 619 Rn. 3 Satz 1, Art. 35 DSGVO.

841 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 35 Abs. 1 S. 1 DSGVO.

842 *Bäcker,* Datenschutz-Grundverordnung, S. 632, Rn. 7, Durchführungspflicht Abs. 1.

843 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 35 Abs. 1 Satz 1 DSGVO.

844 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, S. 623, Rn. 12 Satz 1, Art. 35 Abs. 1 DSGVO.

2.6.2 Verfahren der Datenschutz-Folgenabschätzung

Art. 35 beinhaltet keine detaillierten Vorgaben zur konkreten Durchführung der Datenschutz-Folgenabschätzung. Die in den Abs. 2, 7, 9 und 11 enthaltenen Verfahrensvorschriften beschreiben einen normativen Rahmen, der durch den Verantwortlichen einzuhalten ist und der die Mindestanforderungen an die Operationalisierung der Folgenabschätzung stellt.[845] Die konkrete Durchführung einer Datenschutz-Folgenabschätzung erfolgt auf Grundlage einer eigenen Methodik und Fachlichkeit. Die Herausforderung für Verantwortliche besteht darin, die gesetzgeberische Zielvorstellung in konkrete Datenschutzmanagementmaßnahmen zu „übersetzen" und damit das gesetzgeberische Ziel zu erfüllen.[846] [847]

2.6.2.1 Zeitpunkt

Die Datenschutz-Folgenabschätzung muss als integraler Bestandteil des gesamten Planungs- und Realisierungsprozess eines Datenverarbeitungsverfahrens vor dem Beginn der Verarbeitung personenbezogener Daten durchgeführt werden, wie sich aus dem Wortlaut von Abs. 7 lit. a und Erwägungsgrund 90 ergibt.[848]

In der Praxis bedeutet dies eine enge normative Verflechtung zu den in Art. 25 enthaltenen Anforderungen des Prinzips „Privacy by Design".[849]

Nach Art. 35 Abs. 1 Satz 1 DS-GVO ist die Datenschutz-Folgenabschätzung vorab durchzuführen. Das bedeutet, dass ein Verarbeitungsvorgang nicht in Gang gesetzt werden kann, solange die Ergebnisse seiner Datenschutz-Folgenabschätzung noch nicht feststehen.[850] Empfehlenswert ist es, den Prüfbeginn der Durchführung bereits in den Changemanagement-Prozess eines Verantwortlichen zu integrieren.[851]

---

845 *Datenschutzgruppe 29,* Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, WP 248, S. 19.
846 *Bäcker,* Datenschutz-Grundverordnung, S. 639, Rn. 33.
847 *J. Philipp Albrecht,* Datenschutzrecht, S. 862, Rn. 60, Art. 35 DSGVO.
848 *J. Philipp Albrecht,* Datenschutzrecht, S. 862, Rn. 61.
849 *J. Philipp Albrecht,* Datenschutzrecht, S. 862, Rn. 62, Satz 1.
850 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, S. 505, Rn. 22a, Art. 35 DSGVO.
851 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, S. 786, Rn. 27 Satz 1.

Erwägungsgrund 90

In derartigen Fällen sollte der Verantwortliche vor der Verarbeitung eine Datenschutz-Folgenabschätzung durchführen, mit der die spezifische Eintrittswahrscheinlichkeit und die Schwere dieses hohen Risikos unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und der Ursachen des Risikos bewertet werden. Diese Folgenabschätzung sollte sich insbesondere mit den Maßnahmen, Garantien und Verfahren befassen, durch die dieses Risiko eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden soll.[852]

Eine Datenschutz-Folgenabschätzung muss durchgeführt werden, bevor der zu betrachtende Verarbeitungsvorgang aufgenommen wird. Bei der Aufnahme eines gänzlich neuen Verarbeitungsvorgangs ist zu bedenken, dass die Durchführung einer Datenschutz-Folgenabschätzung, angefangen von der Vorabprüfung hinsichtlich der Notwendigkeit einer Datenschutz-Folgenabschätzung, bis zum Abschluss der Berichtsphase eine gewisse Zeit in Anspruch nehmen kann und nicht ad hoc erstellt werden kann.[853]

Die DS-GVO schreibt nicht vor, wie die innerbetriebliche oder innerbehördliche Organisation aufgestellt sein muss, um die Folgenabschätzung durchzuführen. Auch hierbei lässt sie den Verantwortlichen freie Hand. Allerdings ergeben sich bereits aus den zu erreichenden Zielen methodische Notwendigkeiten, die die innerbetriebliche oder innerbehördliche Organisation prägen. Neben der Unabhängigkeit und hinreichenden Ausstattung muss auch die fachliche Qualifikation der Akteure gewährleistet sein.[854]

2.6.2.2 Altfälle

Für langfristig angelegte Verarbeitungsvorgänge die bereits vor der Geltung der DS-GVO, d.h. vor dem 25.5.2018, (Art. 99 Abs. 1) begannen, besteht grundsätzlich keine Pflicht zur Folgenabschätzung Das entspricht der Grundkonzeption der Vorschrift,

852 Amtsblatt der Europäischen Union 04.05.2016 (Erwägungsgrund 90).
853 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 43144 von 87533, Rn. 105.
854 *J. Philipp Albrecht,* Datenschutzrecht, S. 863, Rn. 66.

künftige Risiken zu antizipieren (Abs. 7 lit. d), statt auf rückwirkende und nachträgliche Bewertungen zu zielen.

Für bereits laufende Verarbeitungsvorgänge ist eine neue Datenschutz-Folgenabschätzung immer dann durchzuführen, wenn sich die Risiken aus den Verarbeitungsvorgängen ändern (Art. 35 Abs. 11 DS-GVO).[855] Da gemäß Erwägungsgrund 171 Satz 3 DS-GVO auf der DSRI[856] beruhende Entscheidungen in Kraft bleiben, bis diese geändert, ersetzt oder aufgehoben werden, ist für Altfälle, bei denen keinerlei Änderungen gegenüber einer seinerzeit durchgeführten Vorabkontrolle nach § 4d Abs. 5 BDSG a.F. vorgenommen wurden, keine Datenschutz-Folgenabschätzung durchzuführen.[857]

Erwägungsgrund 171

Die Richtlinie 95/46/EG sollte durch diese Verordnung aufgehoben werden. Verarbeitungen, die zum Zeitpunkt der Anwendung dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden. Beruhen die Verarbeitungen auf einer Einwilligung gemäß der Richtlinie 95/46/EG, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorliegenden Verordnung fortsetzen kann. Auf der Richtlinie 95/46/EG beruhende Entscheidungen bzw. Beschlüsse der Kommission und Genehmigungen der Aufsichtsbehörden bleiben in Kraft, bis sie geändert, ersetzt oder aufgehoben werden.

2.6.3 Beteiligte einer Datenschutz-Folgenabschätzung, (Art. 35 Abs. 2 DS-GVO)

Nach dem Willen des Verordnungsgebers stellt sich die Durchführung einer Datenschutz-Folgenabschätzung als Managementaufgabe dar, so dass dafür die Unternehmens- oder

855 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, S. 505, Rn. 22a, Art. 35 DSGVO.
856 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates.
857 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, S. 787, Rn. 28 Abs. 2.

Behördenleitung verantwortlich ist.[858] Art. 35 Abs. 1 bis 3, Abs. 7 bis 9 sowie Abs. 10[859] beschäftigen sich mit der Konkretisierung der Pflichten, die den Verantwortlichen bei der Durchführung der Datenschutz-Folgenabschätzung treffen.[860]

Nach Abs. 2 hat der Verantwortliche bei der Durchführung der Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten einzuholen. Es handelt sich hierbei um eine Pflicht des Verantwortlichen, sofern ein Datenschutzbeauftragter bestellt ist. Die Nichtbeachtung dieser Pflicht ist Bußgeldbewehrt.[861]

Die Vorschrift trifft keine Aussage darüber, ob dem Rat des Datenschutzbeauftragten zu folgen ist und begründet erst recht kein bindendes Vetorecht des Datenschutzbeauftragten.[862] Denkbar ist aber, dass die Beachtung bzw. Nichtbeachtung der Einschätzung des Datenschutzbeauftragten im Falle eines Verstoßes gegen die Pflicht der DS-GVO berücksichtigt wird. Hat der Datenschutzbeauftragte etwa eine Einschätzung zu notwendigen Abhilfemaßnahmen abgegeben und folgt der Verantwortliche dieser ohne schlüssige Begründung nicht, könnte dies zu einem höheren Grad der Verantwortung i.S.d. Art. 83 Abs. 2 und in der Folge zu einem höheren Bußgeld führen.[863]

Art. 35 Abs. 2 DS-GVO fordert bei einer Projekt-**DSFA** (**D**aten**s**chutz-**F**olgen**a**bschätzung), den Rat des Datenschutzbeauftragten des Verantwortlichen einzuholen. Im Rahmen einer Datenschutz-Folgenabschätzung kann sich diese Forderung nicht auf die – eventuell sehr vielen – Datenschutzbeauftragten der –vielleicht noch unbekannten – künftigen Verantwortlichen beziehen. Einzelfallabhängig kann es sinnvoll und manchmal sogar geboten sein, den Rat des Datenschutzbeauftragten der für die

858 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, III Beteiligte einer Datenschutz-Folgenabschätzung, Position 43198 von 87533, Rn. 113.

859 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 35 Abs. 1 bis 3, Abs. 7 bis 9 sowie Abs. 10 DSGVO.

860 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, III Beteiligte einer Datenschutz-Folgenabschätzung, Position 43198 von 87533, Rn. 113.

861 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, S. 626 Rn. 18 Abs. 1.

862 *Bäcker,* Datenschutz-Grundverordnung, S. 636 Rn. 18.

863 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, S. 626 Rn. 19.

Erarbeitung des Gesetzentwurfs zuständigen Stelle einzuholen, soweit dieser über die notwendige Sachnähe zur geplanten Verarbeitung verfügt.[864]

Damit scheint die Rollenverteilung abschließend und klar geregelt. Dem Verantwortlichen obliegt die Durchführung der Datenschutz-Folgenabschätzung und der Datenschutzbeauftragte hat einen Beratungs- und Überwachungsauftrag.[865] Zu den Pflichten des Datenschutzbeauftragten gehört es nicht, die Datenschutz-Folgenabschätzung anzustoßen, durchzuführen oder ein Ergebnis zu beurteilen. Im Bereich des Change-Management bspw., wo die Datenschutz-Folgenabschätzung bei wesentlichen Änderungen an der Unternehmens-EDV eine Rolle spielt, dürfte es praxisnah und sinnvoll sein, die Eigentümerschaft weiterhin bei dem Prozess-Owner zu belassen. Die Aufgabenverteilung der DS-GVO sieht nicht vor, dass der Datenschutzbeauftragte proaktiv Nachforschungen über neue Verarbeitungen anstellt oder selbst aktiv wird, um Änderungen in Verarbeitungsvorgängen zu ermitteln.[866]

2.6.4 Regelbeispiele nach Art. 35 Abs. 3 lit. a – c DS-GVO

Abs. 3 lit. a – c[867] enthält eine nicht-abschließende Aufzählung von drei Regelbeispielen von Verarbeitungsvorgängen, für die zwingend vorab eine Datenschutz-Folgenabschätzung durchzuführen ist.[868] Weitere Anhaltspunkte ergeben sich aus Erwägungsgrund 91.

Erwägungsgrund 91

Dies sollte insbesondere für umfangreiche Verarbeitungsvorgänge gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und — beispielsweise aufgrund ihrer Sensibilität — wahrscheinlich ein hohes Risiko mit sich bringen und bei denen entsprechend dem jeweils aktuellen Stand der Technik in

---

864 *Roßnagel / Geminn / Johannes*, Datenschutz-Folgenabschätzung im Zuge der Gesetzgebung, Das Verfahren nach Art. 35 Abs. 10 DS-GVO, in ZD - Zeitschrift für Datenschutz, 435.

865 Zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen, S. 47– 51.

866 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 43243 von 87533, Rn. 118.

867 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Art. 35 Abs. 3 lit. a – c DSGVO.

868 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, S. 626, Rn. 20 Regelbeispiele.

großem Umfang eine neue Technologie eingesetzt wird, sowie für andere Verarbeitungsvorgänge, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, insbesondere dann, wenn diese Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren. Eine Datenschutz-Folgenabschätzung sollte auch durchgeführt werden, wenn die personenbezogenen Daten für das Treffen von Entscheidungen in Bezug auf bestimmte natürliche Personen im Anschluss an eine systematische und eingehende Bewertung persönlicher Aspekte natürlicher Personen auf der Grundlage eines Profilings dieser Daten oder im Anschluss an die Verarbeitung besonderer Kategorien von personenbezogenen Daten, biometrischen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten sowie damit zusammenhängende Sicherungsmaßregeln verarbeitet werden. Gleichermaßen erforderlich ist eine Datenschutz-Folgenabschätzung für die weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen, oder für alle anderen Vorgänge, bei denen nach Auffassung der zuständigen Aufsichtsbehörde die Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, insbesondere weil sie die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern oder weil sie systematisch in großem Umfang erfolgen. Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz- Folgenabschätzung nicht zwingend vorgeschrieben sein.[869]

2.6.4.1 Automatisierte systematische und umfassende Bewertung persönlicher Aspekte

Gem. Art. 35 Abs. 3 lit. a[870] kann eine Datenschutz-Folgenabschätzung erforderlich sein, wenn der Verantwortliche vor der Einführung einer Verarbeitung steht, die eine **automatisierte**, **systematische** und **umfassende Bewertung persönlicher Aspekte**

869 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 91.

870 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 35 Abs. 3 lit. a DSGVO.

ermöglicht. Die Erforderlichkeit leitet sich aber noch nicht aus diesen Umständen selbst ab. Dieses Regelbeispiel verlangt, dass diese Bewertung wiederum gerade als ***Basis*** für **Entscheidungen** genutzt wird, die eine Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen. Diese könnten möglicherweise **Persönlichkeitstests** oder **Scorewertberechnungen** sein. Bei reinen **Mitarbeiterbefragungen**, wie sie bspw. oftmals im Unternehmensumfeld vorkommen, sind in der Regel unmittelbare Rückschlüsse auf einzelne Beschäftigte nicht möglich. Eine Datenschutz-Folgenabschätzung würde sich in diesen Fällen erübrigen.[871]

Fraglich ist, ob die Norm auch Fälle erfasst, in denen der Verantwortliche selbst keine automatisierte Einzelentscheidung trifft. Der Wortlaut der Norm lässt eine solche Auslegung zu, denn danach kommt es nur darauf an, dass der Verantwortliche eine Bewertung persönlicher Aspekte vornimmt, die-von wem auch immer-zur Grundlage für eine Entscheidung gemacht wird.[872]

2.6.4.2 Umfangreiche Verarbeitung von Daten besonderer Kategorien

Das Regelbeispiel des Art. 35 Abs. 3 lit. b 1. Alt.[873] wird bspw. im Bereich des **Arbeitnehmerdatenschutzes** eine Rolle spielen. **Besondere Kategorien** personenbezogener Daten nach Art. 9 Abs. 1 sind häufig Bestandteil in Personalprozessen wie **Arbeitsmedizin** und **Gesundheitsvorsorge** (Gesundheitsdaten) innerhalb des **B**etrieblichen **E**ingliederungs**m**anagements (**BEM**) und adressieren daher oftmals Fragen der Tauglichkeit im Unternehmensumfeld. Daneben zählen zu den besonderen Kategorien personenbezogener Daten Informationen zur rassischen und ethnischen Herkunft, politische Meinungen, **religiöse** oder **weltanschauliche Überzeugung**, **Gewerkschaftszugehörigkeit**, **genetische** und **biometrische Daten** zur eindeutigen Identifikation, **Gesundheitsdaten** und Daten zum **Sexualleben** oder **sexueller Orientierung**.[874] Von der 2. Alt. des Regelbeispiels können bspw. Datenverarbeitungen

---

871 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 42664 von 87533, Rn. 42.

872 *S. Gierschmann,* Systematischer Praxiskommentar Datenschutzrecht (E-Book), 2014, S. 921, Rn. 47, Art. 35 Abs. 3 lit. a DSGVO.

873 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 35 Abs. 3 lit. b 1. Alt. DSGVO.

874 *Gola u. a.* (Hrsg.), Datenschutz-Grundverordnung, S. 299 - 301, Rn. 11 - 13, Art. 9 Abs. 1 DSGVO.

im Zusammenhang mit **Führungszeugnissen** und **Sicherheitsüberprüfungen** berührt sein.[875]

Eine Datenschutz-Folgenabschätzung muss nach Abs. 3 lit. b erfolgen, wenn umfangreiche Verarbeitungen besonderer Kategorien von personenbezogenen Daten nach Art. 9 Abs. 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 verarbeitet werden sollen.[876]

Dies gilt insbesondere bezogen auf **Beschäftigungsverhältnisse,** wo der Umfang mit besonderen Arten personenbezogener Daten sowie mit personenbezogenen Informationen über strafrechtliche Verurteilungen oder Straftaten durch die Rechtsprechung weitgehend limitiert ist.[877]

2.6.4.3 Systematische umfangreiche Überwachung (öffentlich) zugänglicher Bereiche

Eine Datenschutz-Folgenabschätzung soll nach dem Willen des Gesetzgebers auch für die **weiträumige Überwachung öffentlich zugänglicher Bereiche** erforderlich sein. Dies gilt insbesondere, wenn diese mittels **optoelektronischer Vorrichtungen** erfolgt, oder für alle anderen Vorgänge, bei denen nach Auffassung der zuständigen Aufsichtsbehörde die Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, insbesondere weil sie die betroffenen Personen an der **Ausübung eines Rechts** oder der Nutzung einer Dienstleistung bzw. **Durchführung eines Vertrags** hindern oder weil sie **systematisch** in **großem Umfang** erfolgen.[878]

Klassische Beispiele für den **Anwendungsfall** dieses Regelbeispiels stellt die **Videoüberwachung** in Gebäuden wie Einkaufszentren, Bahnhöfen, aber Zügen oder Bussen sowie die systematische Erfassung von Autokennzeichen auf Autobahnen zur Identifikation dar.[879] Was die Definition für den Begriff „öffentlich zugängliche

---

875 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 42664 von 87533, Rn. 43.

876 *Däubler et al.,* EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, S. 473, Rn. 49 Abs. 1.

877 *Däubler et al.,* EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, S. 473, Rn. 51 Satz 1.

878 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 42664 von 87533, Rn. 44.

879 17/ EN WP 248 rev. 01: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk“ for the purposes of Regulation 2016/ 679, S. 9.

Bereiche“ angeht, wird eine Orientierung an der bisherigen Rechtslage und den Anwendungsfällen des BDSG a.F. möglich sein. Es bleibt aber abzuwarten, ob dieser Begriff, genauso wie viele andere, im Laufe der Zeit nicht eine **europäischere Prägung** erhalten wird. Ob bspw. das Areal, welches von verschiedenen Unternehmen geteilt wird, ggf. ein öffentlich zugänglicher Bereich ist, kann in anderen europäischen Ländern möglicherweise anders bewertet werden als in Deutschland.[880]

Vom Anwendungsbereich des Abs. 3 lit. c **ausgenommen** bleiben weiterhin **Betriebsstätten und Betriebe**, die **nicht zum öffentlichen Raum gehören**. Allerdings kann auch in nicht öffentlichen Betrieben eine Verpflichtung zur Durchführung von Datenschutz-Folgenabschätzungen bestehen, wenn die allgemeinen Voraussetzungen in Abs. 1 erfüllt sind. Dies wird mit Blick auf das Kontrollpotenzial von Videokameras und die sich hieraus ableitenden Gefährdungen für Persönlichkeitsrechte regelmäßig der Fall sein.[881]

2.6.5 Positivliste („Backlist“) zur Datenschutz-Folgenabschätzung

Die nationalen Aufsichtsbehörden haben nach Abs. 4[882] eine oder mehrere sog. Positivlisten zu erstellen und zu veröffentlichen. Darin werden Verarbeitungsvorgänge definiert, die nach Auffassung der Aufsichtsbehörden ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen und für die folglich stets eine Datenschutz-Folgenabschätzung durchzuführen ist.[883]

Nachfolgend eine Liste von Verarbeitungsvorgängen nach Artikel 35 Abs. 4 DS-GVO, für die im Zuständigkeitsbereich des **B**undesbeauftragten **f**ür den **D**atenschutz und die **I**nformationsfreiheit (**BfDI**) eine Datenschutz-Folgenabschätzung durchzuführen ist

Version 1.1-BfDI vom 01.10.2019

880 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 42713 von 87533, Rn. 45.
881 *Däubler et al.,* EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, S. 474, Rn. 55.
882 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 35 Abs. 4 DSGVO.
883 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, S. 631, Rn. 27.

Für jede Verarbeitungstätigkeit öffentlicher Stellen des Bundes im Zuständigkeitsbereich des BfDI, für die mindestens zwei der folgenden Merkmale zutreffen, ist eine Datenschutz-Folgenabschätzung gemäß Artikel 35 Absatz 1 DS-GVO erforderlich:

1. Die Verarbeitung umfasst eine Bewertung oder Einstufung der Betroffenen, darunter das Erstellen von Profilen und Prognosen, insbesondere auf der Grundlage von Aspekten, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel der Person betreffen.
2. Die Verarbeitung umfasst eine automatisierte Entscheidungsfindung mit einer Wirkung, die zwar nicht alleine die Grundlage für Entscheidungen mit Rechtswirkung oder ähnlichen bedeutsamen Auswirkungen für die Betroffenen darstellen, aber einen wesentlichen Beitrag zu solchen Entscheidungen liefern.
3. Die Verarbeitung hat die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum Ziel und greift auf beispielsweise über Netzwerke erfasste Daten oder auf eine systematische Überwachung auch nicht öffentlich zugänglicher Bereiche (Artikel 35 Abs. 3 lit. c DS-GVO) zurück.

   a. Bei der Verarbeitung werden vertrauliche oder höchst persönliche Informationen verarbeitet, insbesondere aus den folgenden Kategorien:
   b. Besondere Kategorien personenbezogener Daten nach Artikel 9 Abs. 1 oder Artikel 10 DS-GVO,
   c. Gesundheitsdaten im Sinne des § 67 Absatz 1 SGB X,[884]
   d. Sozialdaten,
   e. Finanzdaten, die umfassende Informationen über die finanziellen Verhältnisse der Betroffenen zulassen, oder die für einen Zahlungsbetrug missbraucht werden können (beispielsweise Kontendaten oder Zahlungsdaten von Konten).

884 Zehntes Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz -, Sozialgesetzbuch X.

4. Es handelt sich um eine Datenverarbeitung in großem Umfang.
5. Im Rahmen der Verarbeitung werden Datensätze aus zwei oder mehreren Verarbeitungen zusammengeführt und/oder abgeglichen, die zu unterschiedlichen Zwecken und/oder von verschiedenen Verantwortlichen durchgeführt wurden, und zwar in einer Weise, die über die vernünftigen Erwartungen der Betroffenen hinausgehen.
6. Bei der Verarbeitung werden Daten zu schutzbedürftigen Betroffenen verarbeitet. Dies umfasst insbesondere die folgenden Gruppen:
   a. Kinder,
   b. Arbeitnehmer / Beamte im Falle einer Verarbeitung durch den Arbeitgeber / Dienstherrn,
   c. Teile der Bevölkerung mit besonderem Schutzbedarf (insbesondere psychisch Kranke, Asylbewerber, Senioren, Patienten),
   d. Betroffene in Situationen, in denen ein besonders ungleiches Verhältnis zwischen der Stellung des Betroffenen und des für die Verarbeitung Verantwortlichen vorliegt.
7. Bei der Verarbeitung werden neue Technologien oder organisatorische Lösungen in einer Art und Weise eingesetzt, die dem gegenwärtigen Stand der Technik voraus ist und deswegen die Abschätzung der Auswirkungen auf die Betroffenen und die Gesellschaft erschwert.
8. Die Verarbeitung an sich hindert die Betroffenen an der Ausübung eines Rechts, der Nutzung einer Dienstleistung oder der Durchführung eines Vertrags. Unabhängig davon können auch Verarbeitungstätigkeiten, bei denen lediglich ein oder sogar kein Kriterium erfüllt ist, ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, so dass grundsätzlich eine Prüfung des Einzelfalles erforderlich ist.

9. Im Übrigen ist zu berücksichtigen, dass die Verarbeitung der folgenden Datenarten in der Regel ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt, so dass insoweit eine Datenschutz-Folgenabschätzung durchzuführen ist:

   a. Umfangreiche Verarbeitung von biometrischen Daten zur eindeutigen Identifikation natürlicher Personen,
   b. Umfangreiche Verarbeitung genetischer Daten,
   c. Umfangreiche Verarbeitung von Daten über den Aufenthaltsort der betroffenen Personen.[885]

2.6.6 Negativliste („White List") der Aufsichtsbehörde

Nach Abs. 5[886] können die zuständigen Aufsichtsbehörden eine „Negativliste" der Verarbeitungsvorgänge erstellen und veröffentlichen, bei denen sie eine Datenschutz-Folgenabschätzung für nicht erforderlich halten.[887]

Problematisch wird die Sachlage allerdings mit der Formulierung „können". Dies impliziert eine Wahlmöglichkeit, die in der Regel nur in bestimmten Fällen vorgenommen wird. Die „Kann-Vorschrift" erlaubt einen größeren Ermessensspielraum als eine „Muss-Vorschrift" oder „Soll-Vorschrift". Dieses ist bei der Anwendung und Interpretation der entsprechenden Artikel der Datenschutz-Grundverordnung zu beachten.

Erstellt eine Aufsichtsbehörde eine Negativliste, so ist auch diese zu veröffentlichen. Es gelten die gleichen Grundsätze, wie bei einer Veröffentlichung nach Abs. 4.

---

885 Liste von Verarbeitungsvorgängen gemäß Artikel 35 Abs. 4 DSGVO für Verarbeitungstätigkeiten öffentlicher Stellen des Bundes (01.10.2019).

886 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 35 Abs. 5 DSGVO.

887 *Däubler et al.,* EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, S. 475, Rn. 60 Satz 1.

Gleichermaßen muss eine Übermittlung dieser Listen an den Europäischen Datenschutzausschuss gemäß Art. 68 DS-GVO erfolgen.[888]

2.6.7 Durchführung (Art. 37 Abs. 7 DS-GVO)

Der **zwingende Mindestinhalt**[889] einer Datenschutz-Folgenabschätzung ist in Art. 35 Abs. 7 DS-GVO vorgegeben. Sie besteht aus vier Elementen, die strukturell aufeinander aufbauen. Darüber hinaus muss der Standpunkt von betroffenen Personen eingeholt, die Durchführung im Rahmen der Rechenschaftspflichten des Verantwortlichen dokumentiert und gemäß Art. 35 Abs. 11 DS-GVO regelmäßig überprüft werden.[890]

Die Dokumentation hat schriftlich zu erfolgen.[891] Neben der Schriftform nach § 126 BGB bzw. der elektronischen Form nach § 126a BGB ist auch die Textform nach § 126b BGB möglich. Den Verantwortlichen trifft in jedem Fall die durch Art. 5 Abs. 2 begründete Nachweispflicht.[892] Die Berücksichtigung der in Abs. 7 lit. a) bis d) aufgeführten Bewertungsschritte ist zwingend aber nicht abschließend.[893]

Der Prozess ist in vier Phasen unterteilt: In der Vorbereitungsphase (1) ist zunächst das geplante Verfahren zur Datenverarbeitung zu beschreiben, das anschließend in der Bewertungsphase (2) aus der Perspektive der Betroffenen zu beurteilen ist. Sodann werden in der Maßnahmenphase (3) Vorkehrungen getroffen, um die identifizierten Risiken einzudämmen. Schließlich werden in der Berichtsphase (4) die Ergebnisse des DSFA-Verfahrens[894] dokumentiert. Die anlassbezogene und regelmäßig erforderliche Fortschreibung der DSFA wird durch die Einbindung in das Datenschutz-Management des Verantwortlichen sichergestellt.[895]

---

888 *Däubler et al.,* EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, S. 476, Rn. 62.
889 *Bäcker,* Datenschutz-Grundverordnung, S. 639, Rn. 32 Satz 1, Art. 35 Abs. 7 DSGVO.
890 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, S. 787, Rn. 30, Art. 35 Abs. 7 DSGVO.
891 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, S. 633, Rn, 31 Satz 1.
892 *Däubler et al.,* EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, S. 477, Rn. 69, Schriftform nach Art. 35 Abs. 7 DSGVO.
893 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, S. 633, Rn. 31, Art. 35 Abs. 7 DSGVO.
894 *Felix Bieker/Marit Hansen/Dr. Michael Friedewald* RDV / Recht der Datenverarbeitung Heft 4/2016, 188 (DSFA - Datenschutz-Folgenabschätzung - Verfahren).
895 *Felix Bieker/Marit Hansen/Dr. Michael Friedewald* RDV / Recht der Datenverarbeitung Heft 4/2016, 188.

Nachfolgende Grafik zeigt den prototypischen Ablauf einer Datenschutz-Folgenabschätzung sehr deutlich auf.

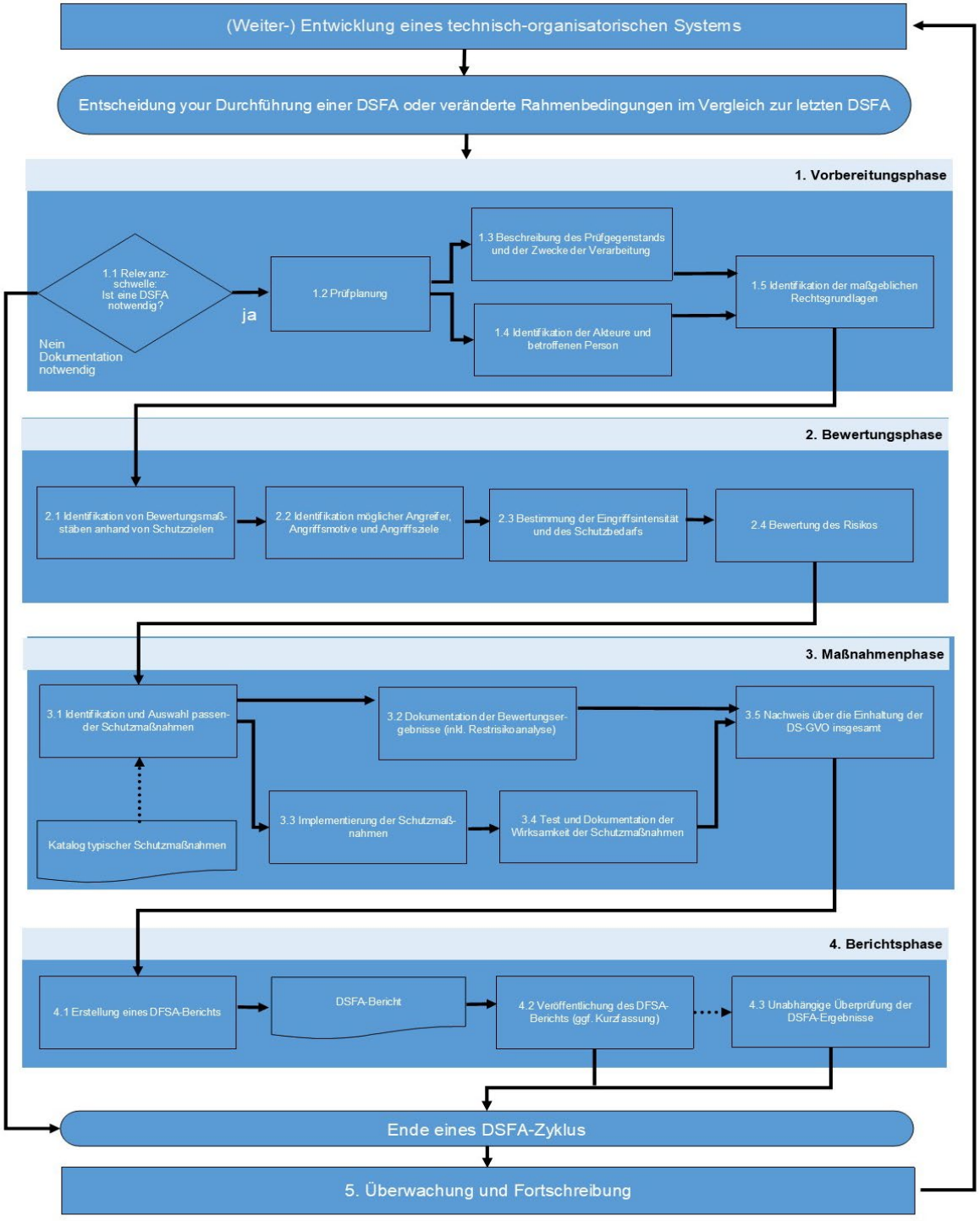

Abbildung 13: Prototypischer Ablauf einer Datenschutz-Folgenabschätzung nach Art. 35 Abs. 7 DS-GVO[896]

896 *Felix Bieker/Marit Hansen/Dr. Michael Friedewald* RDV / Recht der Datenverarbeitung Heft 4/2016, 188.

2.6.8 Überprüfung und Fortschreibung (Art. 35. Abs. 11 DS-GVO)

Abs. 11 verpflichtet den Verantwortlichen, die eigenen Datenverarbeitungen laufend mit den Ergebnissen einer einmal abgeschlossenen Datenschutz-Folgenabschätzung abzugleichen und diese erforderlichenfalls fortzuschreiben oder gar zu wiederholen.[897] Erforderlich ist eine Überprüfung jedenfalls dann, wenn das tatsächliche von dem kalkulierten Verarbeitungsrisiko abweicht. Nach dem Wortlaut der DS-GVO genügt dabei jede „Änderung" des Risikos im Sinne der Risikobewertung nach Abs. 7 lit. c; diese muss nicht substanziell sein.[898]

In Art. 35 Abs. 11, 2. Hs. ist die anlassbezogene Kontrolle geregelt. So könnte z.B. nach einem Hinweis oder einer Beschwerde offenkundig sein, dass vormals festgelegte Abhilfemaßnahmen nicht eingehalten werden oder sich die rechtlichen bzw. tatsächlichen Rahmenbedingungen der Verarbeitung geändert haben.[899]

Art. 35 Abs. 11, 1. Hs.[900] befasst sich demgegenüber mit der turnusmäßigen Kontrolle, die dann konsequenterweise ohne einen konkreten Anlass erfolgt.[901] Hier ist zumindest eine kursorische Prüfung notwendig, um zu beurteilen, ob sich eine Änderung des Risikos ergeben haben könnte. Für die turnusmäßige Kontrolle bietet sich ein Jahresrhythmus an. Maßgebliches Kriterium sollte jedoch nicht die zeitliche Komponente, sondern die tatsächliche Risikoeinschätzung sein.[902]

---

897 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, S. 642, Rn. 52, Überprüfung nach Art. 35 Abs. 11 DSGVO.

898 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Martini, S. 519, Rn. 73.

899 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 43834 von 87533, Rn. 200.

900 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 35 Abs. 11 1. Hs. (1. Halbsatz) DSGVO.

901 *Franck, Lorenz, Dr* PinG - Privacy in Germany Heft 1/2018, 41.

902 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 43834 von 87533, Rn. 201.

2.6.9 Rechtsfolgen und Sanktionen

Die Durchführung einer Datenschutz-Folgenabschätzung ist keine Voraussetzung für die Rechtmäßigkeit einer konkreten Verarbeitung.[903] Eine Datenverarbeitung kann also trotz nicht vorgenommener Datenschutz-Folgenabschätzung rechtmäßig sein. Umgekehrt garantiert die Vornahme der Datenschutz-Folgenabschätzung nicht die Rechtmäßigkeit der Verarbeitung. Das Unterlassen der Durchführung einer **D**aten**s**chutz-**F**olgen**a**bschätzung (**DSFA**) kann allerdings ein Verstoß gegen Art. 25 Abs. 1 (Datenschutz durch Technikgestaltung) begründen.[904]

903 *Körffer et al.,* Bundesdatenschutzgesetz, 10. Aufl. 2010, S. 159, § 4d Rn. 9 und 9a BDSG.
904 *Gola u. a.* (Hrsg.), Datenschutz-Grundverordnung, S. 525, Rn. 73 Abs. 1.

2.7 Datenschutzaudit

Die Regelung freiwilligen Audits stammt aus der Novellierung des BDSG 2001. Die Auditierung im Rahmen freiwilliger Durchführung folgt dem Konzept der Selbstverantwortung, das als Ansatz dem BDSG innewohnt. Audits könnten als eine Stärkung der Rolle des Beauftragten für den Datenschutz gesehen werden.[905] Dass darin auch Konfliktstoff liegt, sei kurz angemerkt: In gewisser Weise wird die Arbeit des Beauftragten mit-auditiert.[906]

2.7.1 Begriff

Der Begriff „Audit" hat seinen Ursprung im Lateinischen:
„audito" – das Hörensagen, Gerede, Gerücht; aber auch die Anhörung
„audire" – anhören, hören, vernehmen.[907]

Ein Audit hat heutzutage jedoch nichts mit den obenstehenden Begriffen zu tun. Ein modernes Audit sollte partnerschaftlich zwischen Auditor und den befragten Personen erfolgen und sicherlich kein „Verhör" darstellen. Eine passende Definition findet sich in „ISO 19011:2011[908] Leitfaden zur Auditierung von Managementsystemen". Demnach ist ein Audit ein: „… systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und zu deren objektiven Auswertung, um zu ermitteln, inwieweit die Auditkriterien erfüllt sind."[909]
Vereinfacht formuliert ist ein Audit daher die Prüfung einer Entität hinsichtlich deren Einhaltung von normierten Anforderungen.[910]

2.7.2 Audit

Die DS-GVO sieht die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und Prüfzeichen vor. Diese sollen dem Nachweis dienen, dass die Vorgabe der DS-GVO bei Verarbeitungsvorgängen von Verantwortlichen oder

905 RDV / Recht der Datenverarbeitung 2000, 95f.
906 *Forgó/Helfrich/Schneider* (Hrsg.), Betrieblicher Datenschutz, S. 275, Rn. 24, Kapitel 6 Datenschutz und Zertifizierung, C. Datenschutzaudit.
907 *Pachinger/Beham,* Datenschutz-Audit, 2017, S. 7 Abschnitt 2.1 Einleitung.
908 Leitfaden zur Auditierung von Managementsystemen (2011).
909 Leitfaden zur Auditierung von Managementsystemen (2011).
910 *Pachinger/Beham,* Datenschutz-Audit, 2017, S. 7 Abschnitt 2.1 Einleitung.

Auftragsverarbeitern eingehalten werden (Art. 42 Abs. 1 DS-GVO). Das Datenschutzaudit nach § 9a BDSG a.F. sah vor, dass sowohl Daten verarbeitende Stellen als auch Anbieter von Datenverarbeitungsprozessen/-programmen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen und können.[911]

Zu Beginn wird im Rahmen eines Initial-Audits der aktuelle Ist-Zustand aller relevanten Bereiche des betrieblichen Datenschutzes im Unternehmen analysiert und bewertet. Auf Basis dieser Erkenntnisse können dann der weitere Projektverlauf systematisch geplant und die einzurichtenden **t**echnischen und **o**rganisatorischen **M**aßnahmen (**TOM**) ausgewählt werden.[912]

Untersucht werden alle datenschutzrechtlich relevanten Unternehmensbereiche, wie beispielsweise die interne IT-Leistungserbringung, das Personalwesen, der Vertrieb, der Einkauf und die Finanzbuchhaltung. Neben diesen gewöhnlich zentral organisierten Funktionsbereichen werden, falls vorhanden, weitere Standorte des Unternehmens in das Audit miteinbezogen. Für diese zusätzlichen Standorte ist jeweils ein eigenes Teil-Audit durchzuführen, für welches eine reduzierte Version des Auditkatalogs verwendet wird.[913]

Der im Anhang befindliche Fragenkatalog ermöglicht eine **Basisauditierung** von Unternehmen zur Feststellung des im Unternehmen bestehenden Datenschutzstandards.

2.7.3 Auditvarianten

Audits können in verschiedene Varianten eingeteilt werden.[914] **Interne Audits,** bei denen meist das Management des Unternehmens der Auftraggeber ist, stellen Erstpartei Audits (First Party Audits) dar. Der Auditor ist ein Mitarbeiter des Unternehmens. Er sollte jedoch aus Unabhängigkeitsgründen nicht Teil des auditierten Bereichs sein.[915]

Externe Audits werden meist von externen Interessierten, also Geschäftskunden, durchgeführt. Diese Zweitpartei-Audits (Second Party Audits) werden beispielsweise

911 *Moos* (Hrsg.), Datennutzungs- und Datenschutzverträge, Hansen-Oest, S. 126, Rn. 2.
912 *Walter,* Datenschutz im Betrieb - DS-GVO in der Personalarbeit, 2018, Position 6628 von 7342, Abschnitt 24.2 Audit, Übung, Wartung.
913 *Walter,* Datenschutz im Betrieb - DS-GVO in der Personalarbeit, 2018, Position 6628 von 7342, Abschnitt 24.2 Audit, Übung, Wartung.
914 Leitfaden zur Auditierung von Managementsystemen (2011).
915 *Pachinger/Beham,* Datenschutz-Audit, 2017, S. 10, Abschnitt 2.2.3 Auditvarianten.

regelmäßig von Automobilherstellern bei deren Zulieferern in den Themenbereichen Qualitätsmanagement oder Informationssicherheitsmanagement durchgeführt. Ein Dilemma stellt dies für Unternehmen dar, bei denen verschiedene Geschäftskunden dasselbe Themengebiet durch Zweitparteien-Audit begutachten lassen.[916]

Eine weitere Variante des ***externen Audits***, welche Abhilfe gegen das Dilemma schaffen könnte, sind die Drittpartei-Audits (Third Party Audit), bei denen eine unabhängige Organisation das Audit durchführt.[917]

2.7.4 Audittypen

Je nach Ziel der Auditierung gibt es unterschiedliche Audittypen, die auch bei der Auditierung des Datenschutzes angewendet werden können:

- Prozessaudit
- Verfahrensaudit
- Produktaudit
- Systemaudit

2.7.4.1 Prozessaudit

Die strukturierte Betrachtung von Prozessen wird von vielen Unternehmen in den einzelnen Geschäftsfeldern praktiziert. Je stärker die Prozessorientierung fortgeschritten ist, umso sinnvoller ist auch die Betrachtung der Prozesse im Rahmen einer Auditierung.[918]

Das Prozessaudit überprüft also bestimmte Vorgänge und Arbeitsabläufe auf systematische Fehler. Ein solches Prozessaudit kann sich dann einfacher darstellen, wenn das Unternehmen bereits über eine fundierte Datenmenge zu den relevanten Prozessen verfügt. Ein systematisches Prozessmanagement kann hierbei helfen. Nicht umsonst ist

916 *Pachinger/Beham,* Datenschutz-Audit, 2017, S. 10, Abschnitt 2.2.3 Auditvarianten.
917 *Pachinger/Beham,* Datenschutz-Audit, 2017, S. 11, Abschnitt 2.2.3 Auditvarianten.
918 *Sachs/Kranig/Gierschmann,* Datenschutz-Compliance nach der DS-GVO, 2017, S. 147 Satz 1 und 2.

ein solches systematisches Prozessmanagement Teil der erweiterten Forderungen der DIN EN ISO 9001 im Qualitätsmanagement.[919]

2.7.4.2 Verfahrensaudit

Nach ISO 9000 besteht ein Unterschied zwischen einem Verfahren und einem Prozess. So lautet die **Definition eines Verfahrens**:

„Festgelegte Art und Weise, eine Tätigkeit oder einen Prozess auszuführen“,

während ein **Prozess** als

„Satz von in Wechselbeziehung oder Wechselwirkung stehenden Tätigkeiten, der Eingaben in Ergebnisse umwandelt“

verstanden wird.[920]

In der praktischen Anwendung wird kein großer Unterschied zwischen einem Verfahrensaudit und einem Prozessaudit mit dem Blickwinkel des Datenschutzes bestehen. Dies ist deswegen der Fall, da ein Prozessaudit mit dem Blickwinkel der Vollständigkeit und Sinnhaftigkeit von Prozessschritten auch den Fokus eines Verfahrensaudits abdeckt, der sich stärker mit der konkreten Umsetzung der Verarbeitungsschritte beschäftigt.[921]

2.7.4.3 Produktaudit

Ein Produktaudit wird immer dann durchgeführt, wenn im Betrieb selbst Fehler an fertigen Produkten festgestellt werden oder durch den Kunden Fehler bei bereits ausgelieferten Produkten reklamiert werden. Es dient also als Managementwerkzeug der unabhängigen Bewertung von Produkten aus Kundensicht und zur Absicherung gegen Produkt- und Sachmängelhaftungsfälle. Die Überprüfung erfolgt mit Hilfe einer der Komplexität und der Fertigungsstückzahl des Produktes angemessenen Stichprobe.[922]

---

919 *International Organization for Standardization*, Qualitätsmanagement ISO 9001, Was ist ein Prozessaudit?, https://www.qualitaetsmanagement.me/iso_9001_audit/prozessaudit/ (zugegriffen am 18032020).

920 *Deutsche Gesellschaft für Qualität*, Audit im Prozesscontrolling, DGQ-Band 13-41, 1999.

921 *Sachs/Kranig/Gierschmann,* Datenschutz-Compliance nach der DS-GVO, 2017, S. 147, Verfahrensaudit.

922 *International Organization for Standardization*, Qualitätsmanagement ISO 9001, Was ist ein Produktaudit?, https://www.qualitaetsmanagement.me/iso_9001_audit/produktaudit/ (zugegriffen am 18032020).

Analog kann mit dem Blickwinkel auf die DS-GVO darunter verstanden werden, dass die Anforderungen der Grundsätze der Verarbeitung sowie den Konkretisierungen wie beispielsweise **Privacy by Design** eingehalten werden.[923]

2.7.4.4 Systemaudit

Bei einem Systemaudit werden stichprobenartig einzelne Bestandteile eines Managementsystems überprüft. Ziel dabei ist, die Konformität gegenüber festgelegten Anforderungen, beispielsweise eines Datenschutz-Managementsystems nachzuweisen.[924]

Basis des Systemaudits ist der Auditfragekatalog, der sich grundsätzlich an der branchenneutralen Normreihe DIN EN ISO 9000:2005[925] orientiert. Das externe Systemaudit kann durch den Kunden selbst (kundenspezifisches Systemaudit) oder durch eine neutrale Zertifizierungsstelle durchgeführt werden. Dabei auditiert die neutrale Zertifizierungsstelle des Qualitätsmanagementsystems eines Unternehmens auf dessen Auftrag hin und vergibt bei Erfüllung der Forderungen nach DIN EN ISO 9001:2008[926] ein Zertifikat.[927]

2.7.5 Auditplan

Die Auditierung der Datenschutzkonformität eines Produktes, eines Verfahrens oder eines Managementsystems wird in der Regel ein recht aufwändiges Projekt sein. Es ist daher üblich, im entsprechenden Verfahren einen sog. Auditplan zu erstellen, aus dem sich der konkrete Ablauf des Audits ergibt. Neben den Inhalten des Audits werden hierin vor allem auch Termine und Abgabezeiten geregelt.[928]

Zuerst sollte das Ziel des Audits definiert werden. Das übliche Ziel eines Datenschutzaudits ist es, die gesetzliche Konformität in Hinblick auf die rechtlichen

---

923 *Sachs/Kranig/Gierschmann,* Datenschutz-Compliance nach der DS-GVO, 2017, S. 147, Produktaudit.

924 *Sachs/Kranig/Gierschmann,* Datenschutz-Compliance nach der DS-GVO, 2017, S. 148, Systemaudit.

925 *International Organization for Standardization*, Qualitätsmanagementsysteme - Grundlagen und Begriffe (ISO 9000:2005), DIN EN ISO 9000:2005, 12.2005.

926 DIN EN ISO 9001:2008-12 (Deutsche Industrie Norm, Europa Norm, International Organization for Standardization), 12.2008.

927 *Kamiske, Gerd F./Brauer, Jörg-Peter*, Qualitätsmanagement von A - Z, Wichtige Begriffe des Qualitätsmanagements und ihre Bedeutung, 2016.

928 *Moos* (Hrsg.), Datennutzungs- und Datenschutzverträge, S. 140 §6 Abschnitt 7, M 6.1.6 Auditplan, a) Ratio.

Vorgaben nachzuweisen[929] In Anlehnung an Ziffer 9. 1. 2 der ISO/IEC 17021-1:2015[930] sieht Absatz 1 vor, dass der Auftragnehmer gemeinsam mit dem Auftraggeber einen **Auditplan** erstellt. Essenzielle Bestandteile des Plans sind dabei die Festlegung der Audittätigkeiten und eine Abstimmung von Terminen.[931]

2.7.5.1 Bestandteile eines Auditplans

Ein Auditplan enthält in Anlehnung an die Vorgaben der ISO/IEC 17021-1:2015-11 folgende Bestandteile:

- Auditziele
- Auditumfang
- Auditkriterien
- Termine
- Terminstandort/Standorte

2.7.5.2 Bereitstellung des Auditplans

Auch wenn Parteien bei der Erstellung des Auditplans zusammenwirken sollen, wird der Auditplan letztlich verantwortlich immer vom Auftragnehmer erstellt werden. Dieser wird nach der in diesem Vertrag vorgesehenen Klausel dem Auftraggeber den Auditplan in Textform, also z.B. per E-Mail zusenden. In der Praxis ist die Zusendung per E-Mail mittlerweile üblich, so dass ein ***Verweis auf die Schriftform hier wenig praxisnah*** erscheint.[932]

2.7.6 Durchführung

Die Durchführung der Audits folgt der Audit-Agenda, die sich wiederum nach den Vorgaben der Audit-Checkliste richtet. Im Rahmen der Durchführung der Audits werden zudem die Audit-Nachweise gesammelt. Ein Audit beginnt mit einem Einstiegsgespräch von Auditoren, anschließend werden die verschiedenen Prüfmethoden unter

929 *Pachinger/Beham,* Datenschutz-Audit, 2017, S. 11, Abschnitt 2.4 Planung eines Audits, Satz 1.
930 Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren, 11.2015.
931 *Moos* (Hrsg.), Datennutzungs- und Datenschutzverträge, S. 140, Rn. 49, b) Erstellung eines Auditplans (Ziffer 6.1).
932 *Moos* (Hrsg.), Datennutzungs- und Datenschutzverträge, S. 141, Rn. 55.

Berücksichtigung der lokalen Besonderheiten (etwa Einschränkungen durch Remote-Audits) angewandt und schließlich der Audit formell beendet.[933]

Folgende Schritte haben sich dabei bewährt:

- Eröffnungsgespräch (formaler Beginn des Audits)
- Durchführung anhand verschiedener Auditmethoden
- Beendigung des Audits (formelles Ende des Audits)[934]

2.7.6.1 Eröffnungsgespräch

Das Eröffnungsgespräch findet am ersten Audittag zu Beginn des Audits statt.[935] Im Regelfall beginnt der Audit mit einem kurzen Kennenlernen von Auditoren und Auditees. Die Beteiligten stellen sich untereinander vor, die Auditoren erläutern noch einmal die Vorgehensweise und das Ziel der Audits – die Überprüfung der Wirksamkeit des DSMS (Datenschutzmangementsystem) im auditierten Bereich.[936] Es ist angeraten, für diesen Zweck eine Checkliste zu verwenden, die darüber hinaus als Grundlage für das eigentliche Audit dienen kann.

933 *Loomans/Matz/Wiedemann,* Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, 2014, S. 195, Abschnitt 5.2.9.2.
934 *Sachs/Kranig/Gierschmann,* Datenschutz-Compliance nach der DS-GVO, 2017, S. 154, Abschnitt 9.2.4.2.
935 *Pachinger/Beham,* Datenschutz-Audit, 2017, S. 17 Abschnitt 2.5.1.
936 *Loomans/Matz/Wiedemann,* Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, 2014, S. 197.

Checkliste: Eröffnungsgespräch Datenschutz-Audit

Themen	Bemerkungen
Vorstellung der Parteien	
Auditteamleiter	
Auditoren	
Leitung (Geschäftsführer oder Bereichsleiter)	
Datenschutzverantwortliche	
Rechts-/Complianceleiter	
Betreuer (Guide)	
Auditauftraggeber	
Kurze Vorstellung des Unternehmens	
Ziel des Audits	
Besprechung Auditumfang (Scope); Bestätigung, dass die vom Auditteam benötigten Ressourcen und Einrichtungen zur Verfügung stehen	
Feinabstimmung des Auditplans	
Auditmethodik (Dokumente lesen, Interviews, Beobachtungen)	
Methoden der Berichterstattung einschließlich der Einstufung der Auditfeststellungen	
Abstimmen des offiziellen Kommunikationsweges	
Hinweis auf Zwischenabstimmung und das Abschlussgespräch	
Informationen zu den Bedingungen, die zum vorzeitigen Abbruch eines Audits führen können	
Beantwortung offener Fragen	

Abbildung 14: Checkliste Eröffnungsgespräch Datenschutz-Audit

2.7.6.2 Prüfmethoden

Die wichtigste Prüfmethode stellen die Interviews der Auditees dar. Bei diesen Interviews ist die psychologische Komponente von großer Bedeutung, es handelt sich bei einem Audit schließlich immer um eine Testsituation.[937]

937 *Loomans/Matz/Wiedemann,* Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, 2014, S. 196, Abschnitt 5.2.9.2.2.

Bei **Interviews** (einzelner Auskunftspersonen) kann sich der Auditor auf sein Gegenüber konzentrieren. Mehrere Interviews zum selben Thema mit unterschiedlichen Auskunftspersonen ergeben ein objektiveres Bild über die tatsächlichen Abläufe.[938]

Weiterhin werden stichprobenhaft **Dokumente und Aufzeichnungen eingesehen**. Dies betrifft neben inhaltlichen Aspekten (Angemessenheit der ADV-Regelungen) auch formelle Aspekte, besonders wichtig ist die Überprüfung einer angemessenen Dokumentenverwaltung. Dabei ist nicht nur zu prüfen, ob Unterlagen entsprechend den Vorgaben der Organisation verwaltet werden, sondern auch, ob diese Vorgaben den Audit-Kriterien entsprechen. Als Audit-Nachweis sind neben Notizen Kopien der einschlägigen Unterlagen möglich, meist reicht jedoch ein entsprechender Verweis aus.[939]

Zur Durchführung von Datenschutzaudits werden regelmäßig Vor-Ort-Prüfungen erforderlich sein, um den durch Dokumentationen des Auftraggebers aufgezeichneten Stand mit der praktischen Umsetzung abzugleichen.[940] Für den Datenschutz insbesondere relevant sind hier die Betrachtung der Arbeitsplätze (u.a. Clean Desk), der PCs (Passwortschutz), der Kopierer und Drucker (Vertrauliche Dokumente im Ausgabefach), der Papierkörbe (Vertrauliche Dokumente nicht adäquat vernichtet), Serverräume und Rechenzentren (Zutrittsschutz), des Empfangsbereich (Videoüberwachung) etc. Der Auditor muss anhand der Audit-Checkliste jeden geprüften Sachverhalt notieren. Als Audit-Nachweis kommen hier neben Notizen auch Fotos, Screenshots, Auszüge aus Protokolldateien etc. in Frage.[941]

2.7.6.3 Beendigung

Zum Ende des Audits kommen Auditoren und Auditees zu einer gemeinsamen Schlussrunde zusammen, in welcher der Audit formell für beendet erklärt wird. Der Auditor bedankt sich für die Teilnahme der Auditees und stellt die weitere Vorgehensweise und den Zeitrahmen vor. Eventuelle Unklarheiten und Missverständnisse zwischen den Parteien werden spätestens zu diesem Zeitpunkt

938 *Pachinger/Beham,* Datenschutz-Audit, 2017, S. 19 Abs. 3 Satz 2.
939 *Loomans/Matz/Wiedemann,* Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, 2014, S. 196, Abschnitt 5.2.9.2.2.
940 *Moos* (Hrsg.), Datennutzungs- und Datenschutzverträge, S. 143, Rn. 64.
941 *Loomans/Matz/Wiedemann,* Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, 2014, S. 197 und 198, Begehung der Räumlichkeiten.

ausgeräumt. Die Parteien gehen zur Nachbereitung der Audits auseinander, wobei sich das ausführlichere Abschlussgespräch[942] häufig direkt anschließt.[943]

Das Abschlussgespräch bildet den offiziellen Abschluss eines Audits, also das Ende des geplanten Audits nach Auditplan. Es dient der unmittelbaren Kommunikation der Auditergebnisse an die Leitung des auditierten Bereiches, die Verantwortlichen für Prozesse und Verfahren und die Auskunftspersonen.[944]

2.7.6.4 Nachbereitung

Audit-Feststellung und Ableiten der Audit-Schlussfolgerungen auf Basis der Audit-Nachweise kann der Auditor meist sehr schnell feststellen, inwieweit ein Audit-Kriterium erfüllt worden ist oder nicht. Zu unterscheiden ist zwischen vier verschiedenen Feststellungsarten:

1) Kritische Abweichung
2) Nebenabweichung
3) Beobachtung
4) Best Practices

Die Auditfeststellungen sollten in der dem Audit folgenden Zeit durch Implementierung von Maßnahmen behoben werden. Hierzu sollte mit den Auditoren ein abgestimmter Maßnahmenumsetzungsplan erstellt werden. Die Wirksamkeit der umgesetzten Maßnahmen sollte in Folgeaudits, die im Einklang mit dem Auditprogramm stehen, überprüft werden. Erst nach dieser Wirksamkeitsbewertung einer Maßnahme wird die Auditfeststellung im Abweichungsbericht geschlossen.

942 Leitfaden zur Auditierung von Managementsystemen (2011).
943 *Loomans/Matz/Wiedemann,* Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, 2014, S. 198, Abschnitt 5.2.9.2.3.
944 *Pachinger/Beham,* Datenschutz-Audit, 2017, S. 23, Abschnitt 2.5.5 Abschlussgespräch.

Die nachfolgende Grafik zeigt den Zusammenhang der einzelnen Bereiche auf und in welcher Phase sie von Bedeutung sind.

Abbildung 15: Kausalkette Audit[945].

945 *Loomans/Matz/Wiedemann,* Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, 2014, S. 179, Abb. 5.2.3 Kausalkette der Audit-Begriffe im Datenschutzmanagement Audit.

2.8 Changemanagement

Die ersten Analysen haben aufgezeigt, dass die Fortführung des „Status Quo“ keine zielführenden Ergebnisse produzieren würden. Die Umstellung bzw. Einführung der doch sehr komplexen Datenschutz-Grundverordnung, auf bestehendem Level als einfache Zusatzarbeit deklariert, würde so nicht umgesetzt werden können. In der Konsequenz war es erforderlich, dass die deutsche Gesellschaft einen Veränderungsprozess durchmachen müsse. Aus diesem Grund wurde die Entscheidung getroffen, den Unternehmenswandel, durch ein „Change-Management“ herbeizuführen.

Die technologischen Entwicklungen führen zu einer unerhörten Beschleunigung aller Geschäftsabläufe und stellen die gesamte Geschäftswelt unter einen gewaltigen Leistungs- und Veränderungsdruck.[946]

2.8.1 Begriff

Nichts ist so beständig wie der Wandel, wird gemeinhin gesagt. Für die Wirtschaftswelt gilt dies fraglos und in zunehmenden Maßen – und damit auch für die einzelnen Unternehmen, die eine zentrale Stellung darin einnehmen.[947]

Für spezielle Managementtechniken, die zur Steuerung der Prozesse von Wandel selbst erforderlich sind, hat sich dabei der Begriff ***Change-Management*** eingebürgert.[948]

Laufende Anpassung von Unternehmensstrategien und -strukturen an veränderte Rahmenbedingungen. Wandel repräsentiert heute in Unternehmen nicht mehr den Sondervorgang, sondern eine häufig auftretende Regelerscheinung. Alle Prozesse der globalen Veränderung, sei es durch Revolution oder durch geplante Evolution, fallen in das Aufgabengebiet des Change-Managements.[949]

2.8.2 Durchführen organisatorischer Veränderungen

Zukunftssichernde strategische und unternehmenspolitische Entscheidungen werden in den kommenden Jahren vermehrt zur Verlagerung von Aufgaben und zu neuen

946 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, Rahmenbedingungen, Nr.2, S. 24 Abs. 1.
947 *Lauer,* Change Management, 2. Aufl. 2014, Begriff Change Mangement, S. 3, Satz 1.
948 *Lauer,* Change Management, 2. Aufl. 2014, Begriff Changemanagement, S. 3+4.
949 *Gabler Wirtschaftslexikon*, https://wirtschaftslexikon.gabler.de/definition/change-management-28354/version-251986.

Schnittstellen in der Organisation führen – oft mitten durch die einzelnen Betriebe und bis hinunter an die Basis: Umgestaltung der Produktpalette; Reduktion von Verwaltungsaufwand; Verflachung der Hierarchie; Schaffen ergebnisverantwortlicher Geschäftsbereiche; Dezentralisierung im Hinblick auf Markt- und Kundennähe; Fusionen, Kooperationen und Joint Ventures; Verlagerung von Aktivitäten in andere Länder.

Jede dieser Entscheidungen bedeutet, dass Massen von Führungskräften aller Stufen während eines halben oder ganzen Jahres zweierlei gleichzeitig bewältigen müssen: die Aufrechterhaltung des Normalbetriebs – und die Umstrukturierung ihrer Organisationseinheit. Die Führung des normalen Geschäfts – das hat man im günstigsten Fall noch gelernt, obwohl auch hier nicht jeder aus dem Vollen schöpft. Vor einer Reorganisation im eigenen Verantwortungsbereich aber stehen heute viele zum ersten Mal in ihrem Leben. Ein solches Projekt erfordert besondere Mechanismen der Planung, Steuerung, Kommunikation und Führung und in personellen Fragen ist äußerste Umsicht und Sorgfalt gefragt, wenn das Tagesgeschäft einigermaßen normal über die Bühne und im klimatischen Bereich nicht allzu viel Porzellan in die Brüche gehen soll. Dies alles immer unter einem enormen Zeit- und Leistungsdruck. Da ist manch einer – als Mensch und als Manager – schlicht überfordert.[950]

2.8.3 Leistung erzeugen durch Synergie

Die Kunst der Führung besteht heute zunehmend darin, mit Ressourcen, die auch der Konkurrenz zur Verfügung stehen, durch Synergieeffekte eine höhere Gesamtleistung zu erzielen. Dies hängt unter anderem von den Strukturen ab: Die Aufgaben müssen sinnvoll gebündelt sein. Es hängt aber auch, entscheidend sogar, vom Verhalten der Menschen ab – davon, wer mit wem in welcher Art und Weise kommuniziert und kooperiert. Dies gilt für das Zusammenspiel im Rahmen einer Konzernorganisation genauso wie für das Zusammenspiel von Mitarbeitern und Arbeitsgruppen im Betrieb. Darauf Einfluss zu nehmen ist eine Kernfunktion der Führung.[951]

---

950 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, Durchführung organisatorischer Veränderungen, S. 44.

951 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, Leistung erzeugen durch Synergien, S. 47.

2.8.4 Neue Aufgaben – neue Strukturen

Wenn Zeit und Geld knapp werden und gleichzeitig die Komplexität zunimmt, kann man nicht mehr so weiterwirtschaften wie in der Vergangenheit. Die Herausforderung für das einzelne Unternehmen lautet:

- schnellere und wirtschaftlichere Bewältigung
- einer zunehmenden Vielfalt
- sich rasch ändernder Aufgaben.[952]

2.8.5 Überlebensstrategie und Zukunftssicherung

Zeitdruck, tendenzielle Überlastung, Gefahr der Überforderung und gleichzeitig die Notwendigkeit, neue Aufgaben zu übernehmen und neue Fertigkeiten zu erwerben – all dies unter einen Hut zu bringen ist für Mitarbeiter und Führungskräfte nur in einem Umfeld möglich, in dem ein einigermaßen angstfreies Klima herrscht, einem Umfeld, in dem man auch über persönliche Erfahrungen, eigene Unsicherheiten und berufliche Schwierigkeiten miteinander spricht: in einer offenen und lebendigen, partnerschaftlichen und teamorientierten Führungskultur. Nun wird leider »Unternehmenskultur« mancherorts immer noch als Modetrend oder Luxusartikel betrachtet. In Wahrheit geht es hierbei aber nicht einfach um individuelle Lebensqualität im Arbeitsbereich. Es geht vielmehr um Fragen, die für die Zukunft des Unternehmens von entscheidender Bedeutung sind, nämlich

- ob die Probleme im Unternehmen rechtzeitig erkannt und gelöst werden. Eine offene und lebendige Unternehmenskultur, in der kritisch gedacht und gesprochen wird, ist das beste Frühwarnsystem, das es gibt;
- ob Mitarbeiter und Führungskräfte sich mit dem Unternehmen identifizieren und sich für den gemeinsamen Erfolg engagieren, oder ob sie einfach »jobben« und bei der ersten sich bietenden Gelegenheit abwandern – eine Frage, die relevant ist für den Aufbau und die Erhaltung von Know-how im Unternehmen;

952 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, Neue Aufgaben-neue Strukturen, S. 60, Abs. 1.

- vor allem: ob, wie rasch und wie konsequent Managemententscheidungen sowie organisatorische Veränderungen im Betrieb umgesetzt werden können – angesichts des raschen Wandels die Gretchenfrage.[953]

2.8.6 Management von Veränderungen in Organisationen

Veränderungsprojekte in Organisationen sind heute an der Tagesordnung, doch sie funktionieren nur, wenn alle Beteiligten davon überzeugt sind, dass sich etwas ändern muss. Hier ist Überzeugungsarbeit zu leisten um alle Betroffenen „mit zu nehmen". Nachfolgende Übersicht ermöglicht einen groben Einblick in den Bereich des Veränderungsmanagements von Organisationen.

Organisationsentwicklung (OE)

Diese sind meistens mittel- bis langfristig angelegt

Begriff für »**geplanten Wandel**« (von engl. Organisation Development, Planned Change)

»Bereichsentwicklung«: OE in einzelnen Organisationseinheiten

⇨ Primat des Transfers: Schaffen optimaler Voraussetzungen für die Umsetzung

⇨ Entwicklung als Veränderungsprinzip: (Strukturen, Menschen, Führungskultur)

⇨ Ganzheitliches Organisationsverständnis: Gleichgewichtige Berücksichtigung der harten Faktoren (Strukturen, Finanzen, Führungssysteme) und der weichen Faktoren (Kommunikation, Führung, Zusammenarbeit)

⇨ Partizipation: Situatives und stufengerechtes Einbeziehen der betroffenen Führungskräfte und Mitarbeiter/-innen

⇨ Prozessorientierte Steuerung: Konstruktiver Umgang mit Widerständen und Konflikten

⇨ Hilfe zur Selbsthilfe: Wissensvermittlung, Training, Moderation, Coaching, Beratung

953 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, Überlebensstartegie und Zukunftssicherung, S. 69 +70.

Generelle Tempobeschleunigung: Klassische Organisationsentwicklung ist heute nur noch in Ausnahmefällen möglich.[954]

Change-Management

Change-Management wird meistens kurz- bis mittelfristig angelegt

Umgangssprachlich moderner Sammelbegriff für alles, was heutzutage an Veränderungen in Organisationen praktiziert wird (nicht Bezeichnung für eine bestimmte Veränderungsstrategie)

⇨ Schwerpunkte: M&A, Restrukturierungen, Auslagerungen, Sanierungen, Kostensenkungsprogramme, Geschäftsprozessoptimierung

⇨ zumeist enormer Zeitdruck (in einzelnen Fällen sachlich begründet, häufig jedoch lediglich Ausfluss dysfunktionaler Managementhektik)

⇨ unter der Ägide großer Beratungsfirmen (z.B. McKinsey, Accenture, KPMG etc.): Vorwiegend technokratisches Vorgehen einseitig betriebswirtschaftlich orientierter Berater mit entsprechenden Streuverlusten und Kollateralschäden im personellen und kulturellen Bereich Nachhaltiger Erfolg setzt nach wie vor Leadership sowie prozessorientierte Vorgehensweisen voraus.[955]

Die Methoden, die in erfolgreichen Transformationen genutzt werden, basieren alle auf einer grundlegenden Einsicht: Tief greifender Wandel kann aufgrund einer langen Liste von Gründen leicht scheitern.[956]

Um effektiv zu sein, muss eine Methode, die darauf abzielt, Strategien zu verändern, Prozesse zu reorganisieren oder Qualität zu optimieren, diese Hindernisse angemessen adressieren.[957]

954 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, Managment von Veränderung im Prozess, S. 99+100.
955 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, Change-Management, S. 100.
956 *Kotter,* Leading change, 2015, Der Acht-Stufen-Prozess des Wandels, S. 17.
957 *Kotter,* Leading change, 2015, ebenda, S. 17.

2.8.7 Der Acht-Stufen-Prozess des Wandels

Der Prozess besteht aus acht Stufen, von denen jede mit einem der acht grundsätzlichen Fehler durch die Transformationsbemühungen verhindert werden können, im Zusammenhang steht. Die einzelnen Schritte lauten:

- Erzeugung eines Dringlichkeitsgefühls,
    - Untersuchung der Markt – und -Wettbewerbsrealitäten
    - Identifizierung und Diskussion von Krisen, potenziellen Krisen und grundsätzliche Chancen[958]
- Aufbau einer Führungskoalition
    - Zusammenstellung einer Gruppe mit ausreichender Kompetenz, um den Wandel zu führen
    - Die Gruppe zur Teamarbeit motivieren[959]
- Entwicklung von Visionen und Strategien,
    - Eine für den Wandel richtungsweise Vision schaffen
    - Strategien für die Umsetzung der Vision entwickeln[960]
- Kommunikation der Vision des Wandels,
    - Kommunikation der neuen Vision und der Strategie durch alle Kommunikationskanäle
    - Die Vision muss den Mitarbeitern von der Führungskoalition vorgelebt werden[961]
- Verantwortung auf breite Basis stellen,
    - Hindernisse beseitigen
    - Änderungen von Systemen oder Strukturen, die der Vision des Wandels nicht entsprechen

---

958 *John P. Kotter* Havard Business Manager März / April 1995 (Der Acht-Stufen-Prozess für Umsetzung tief greifenden Wandels, Punkt 1, S. 18).

959 *John P. Kotter* Havard Business Manager März / April 1995 (Der Acht-Stufen-Prozess für Umsetzung tief greifenden Wandels, Punkt 2, S. 18).

960 *John P. Kotter* Havard Business Manager März / April 1995 (Der Acht-Stufen-Prozess für Umsetzung tief greifenden Wandels, Punkt 3, S. 18).

961 *John P. Kotter* Havard Business Manager März / April 1995 (Der Acht-Stufen-Prozess für Umsetzung tief greifenden Wandels, Punkt 4, S. 18).

    - Zur Risikobereitschaft und zu ungewöhnlichen Ideen, Aktivitäten und Handlungen ermutigen[962]
- Schnelle Erfolge erzielen,
    - Sichtbare Leistungsverbesserungen oder „Erfolge“ planen
    - Diese Erfolge erreichen
    - Die Menschen, die diese Erfolge ermöglichten, für alle deutlich anerkennen und auszeichnen[963]
- Diese Erfolge konsolidieren und weitere Veränderungen einleiten,
    - Die wachsende Glaubwürdigkeit dazu nutzen, alle Systeme, Strukturen und Verfahren zu verändern, die nicht zusammenpassen und nicht der Vision des Wandels entsprechen
    - Menschen, die die Vision des Wandels umsetzen können, einstellen, befördern und entwickeln
    - Den Prozess mit neuen Projekten, Themen und Change Agents wiederbeleben[964]
- Neue Ansätze in der Kultur verankern.
    - Erreichung einer Leistungsverbesserung durch kunden- und produktivitäts-orientiertes Verhalten, mehr und bessere Führung und effektives Management[965]
    - Die Beziehung zwischen neuem Verhalten und Unternehmenserfolg herausstellen
    - Maßnahmen entwickeln, die Führungsentwicklung und – nachfolge sicherstellen.[966]

962 *John P. Kotter* Havard Business Manager März / April 1995 (Der Acht-Stufen-Prozess für Umsetzung tief greifenden Wandels, Punkt 5, S. 18).
963 *John P. Kotter* Havard Business Manager März / April 1995 (Der Acht-Stufen-Prozess für Umsetzung tief greifenden Wandels, Punkt 6, S. 18).
964 *John P. Kotter* Havard Business Manager März / April 1995 (Der Acht-Stufen-Prozess für Umsetzung tief greifenden Wandels, Punkt 7, S. 18).
965 *John P. Kotter* Havard Business Manager März / April 1995 (Der Acht-Stufen-Prozess für Umsetzung tief greifenden Wandels, Punkt 8, S. 18).
966 *John P. Kotter* Havard Business Manager März / April 1995 (Havard Business Manager).

2.8.8 Die wesentlichen Punkte

Um Genaueres über die Ausgangssituation zu erfahren, müssen folgende Punkte überprüft werden:

- **Klarheit der Ziele**: Wie klar ist den Betroffenen, was mit dieser Veränderung konkret bezweckt wird? Die Frage ist nicht: Wie klar ist sie dem, der sie vorantreiben will? **Sondern**: Wie klar, wie konkret und wie einsichtig ist die Zielsetzung für die Betroffenen – aus ihrer Perspektive, von ihrem Standort aus gesehen? Können sie sich konkret vorstellen, was nachher anders sein wird als heute? Oder fühlen sie sich nur mit inhaltsleeren Worthülsen zugeschüttet?
- **Informationsstand**: Von welchem Wissensstand über das anstehende Thema kann man ausgehen? Gibt es diesbezüglich gravierende Unterschiede? Was wissen die Betroffenen über die Art und Weise, wie das Vorhaben entstanden ist, von wem die Idee ausging, was oder wer sonst noch dahintersteckt?
- **Problembewusstsein**: Empfinden die Betroffenen die Situation, um die es geht, überhaupt als Problem? Gibt es so etwas wie »Leidensdruck«? Wie weit ist dieser verbreitet? Hat man sich eventuell längst mit der Situation arrangiert, sieht mittlerweile darin sogar Vorteile? Und: Wie offen wird darüber geredet?
- **Glaubwürdigkeit des Vorhabens und der Initianten**: Wie sehr nimmt man den Initiatoren ab, dass es ihnen tatsächlich um die Sache geht, die sie vorbringen? In welchem Ausmaß unterschiebt man ihnen verdeckte, eventuell eigennützige Motive? Glaubt man, dass sie an einem gemeinsamen Vorgehen interessiert sind? Wie verbreitet sind Vermutungen, es handle sich um eine reine Alibi-Übung oder um einen Manipulationsversuch?
- **Energie und Engagement**: Aus alldem ergibt sich das Ausmaß an Energie, mit dem sich die Beteiligten für die Problemanalyse und -lösung engagieren oder sich gegen sie sperren werden.[967]

Erst wenn man spürt, dass die Betroffenen die Probleme erkennen und dass der Impuls zum kreativen Mitmachen vorhanden ist, macht es Sinn, den nächsten Schritt zu tun, das heißt in die Phase der konkreten Problembearbeitung überzuleiten.

---

967 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, Die wesentlichen Punkte, S. 117.

Dies alles kann selbstverständlich nur auf der Basis eines offenen und sensiblen Dialogs mit den Betroffenen gelingen. Klar auch: Je nachdem, wo und an wie unterschiedlichen »Standorten« die Betroffenen sich befinden, muss wenig oder sehr viel Zeit einkalkuliert werden, um die Beteiligten miteinander sowie mit dem Thema, um das es geht, in Kontakt zu bringen, sie dialogbereit und die Dinge „besprechbar“ zu machen.[968]

2.8.9 Strategieentwicklung

Der Duden (Bedeutungswörterbuch) erklärt den Begriff wie folgt:

„genauer Plan für ein Verhalten, der dazu dient, ein (militärisches, politisches, psychologisches o. ä.) Ziel zu erreichen, und in dem man alle Faktoren von vornherein einzukalkulieren versucht: eine Strategie festlegen, anwenden; sich eine Strategie für eine Verhandlung überlegen… “[969].

So wie das Unternehmertum innerhalb des Unternehmens nicht ohne unternehmerisches Management, das heißt ohne interne Verfahren und Methoden funktionieren kann, ist es auf dem Markt auf Verfahren und Methoden angewiesen.[970]

Die Informationen und Daten aus dem externen und internen Umfeld sowie die Erkenntnisse aus der Stärken- und Schwächenanalyse (SWOT) bilden die Basis für die Entwicklung von Zielen und Strategien.[971]

968 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, Die wesentlichen Punkte, S. 117.
969 *Dudenredaktion,* Das Bedeutungswörterbuch, 5. Aufl. 2018, S. 928, Strategie.
970 *Drucker/Gebauer/Simon,* Was ist Management?, 7. Aufl. 2014, S. 196, Abschnitt 12. Strategien des Entrepreneurs, Abs. 1 Satz 1.
971 *Wagner,* Strategie und Managementwerkzeuge, 2007, S. 45 Satz 1, Abschnitt 3. Strategieentwicklung.

Nachfolgende Abbildung zeigt eine einfache Übersicht über die Stärken Schwächenanalyse (SWOT)[972] auf

S - **S**trengths W - **W**eaknesses O - **O**pportunities T - **T**hreats		Interne Analyse, Merkmale des Unternehmens	
		Stärken **Strengths**	Schwächen **Weaknesses**
Externe Analysen, Entwicklungen	Gelegenheiten Möglichkeiten Potenziale Chancen **Opportunities**	Ausbauen	Aufholen
	Bedrohung Gefahren **Threats**	Absichern	Vermeiden

Abbildung 16: Übersicht strategische Stoßrichtungen nach SWOT[973]

Die strategische Planung sollte nicht nur mit einem Jahreshorizont erfolgen, sondern sie sollte auch langfristig angelegt sein. Um eine gewisse Planungssicherheit zu erlangen, stellt man für die langfristige Planung unterschiedliche Szenarien auf.[974]

Für eine Planungsperiode von einem Jahr lassen sich Umfeldfaktoren, wie Inflationsrate in Deutschland oder Wechselkurse, noch mit relativ hoher Sicherheit bestimmen.[975] Bei einer in Europa geltender Datenschutz-Grundverordnung (DS-GVO) ist dies am heutigen Tage nur eingeschränkt möglich. Es handelt sich hierbei schließlich um eine Verordnung, welche an ihrer Praxistauglichkeit gemessen werden wird. Hierzu wird in der

---

972 *Gabler Wirtschaftslexikon*, SWOT Analyse, dt. Abk. für Analysis of strengths, weakness, opportunities and threats, https://wirtschaftslexikon.gabler.de/definition/swot-analyse-52664/version-275782.

973 *B-wise GmbH*, Wofür braucht es eine SWOT-Analyse, https://www.business-wissen.de/hb/wofuer-braucht-es-eine-swot-analyse/.

974 *Wagner,* Strategie und Managementwerkzeuge, 2007, S. 45, Abschnitt 3. Strategieentwicklung.

975 *Wagner,* Strategie und Managementwerkzeuge, 2007, S. 47, Abschnitt 3.1 Szenarien.

nachfolgenden Abbildung ein realer Ablauf bezüglich des Entwickelns von Szenarien aufgezeigt.

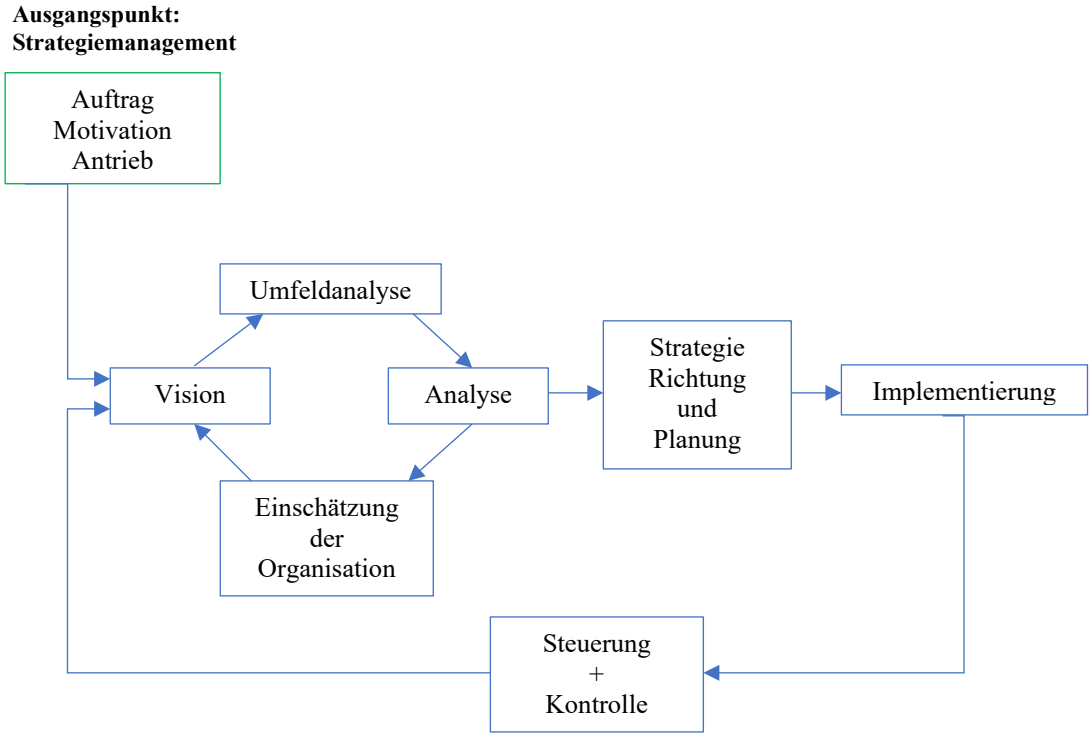

Abbildung 17: Der reale Ablauf des Entwickelns und Anwendens von Szenarien[976]

976 *Pillkahn, Ulf*, Trends und Szenarien als Werkzeuge zur Strategieentwicklung, Wie Sie die unternehmerische und gesellschaftliche Zukunft planen und gestalten, 2007.

2.8.10 Instrumente und Verfahren der Unternehmensentwicklung

Im Prinzip steht eine fast verwirrende Vielfalt von Methoden, Instrumenten und Verfahren zur Verfügung, um die Entwicklung eines Unternehmens voranzutreiben. Zur besseren Orientierung werden bei der folgenden Gesamtübersicht folgende Ordnungskategorien verwendet:

- Adressat der Maßnahme (Intervention)
    - der Einzelne
    - die Gruppe
    - das gesamte Unternehmen oder wesentliche Teile
    - relevante Umwelten des Unternehmens
- Art der Maßnahme (Intervention)
    - eher über weiche Faktoren
    - (Wissen und Können, Einstellungen und Verhalten)
    - eher über harte Faktoren
    - (Strukturen und Abläufe, Systeme und Regelungen)

Es existieren Instrumente und Verfahren, bei denen eine eindeutige Zuordnung schwerfällt, da diese sowohl bei harten als auch bei weichen Faktoren ansetzen.[977] Nachfolgende Abbildung ermöglicht eine Auswahl analog eines Besuchs in der Cafeteria. Was immer für das Management von Veränderung (Changemanagement) besonders zweckdienlich erscheint kann verwendet und ausgewählt werden. Wobei einiges **selbstverständliches Handwerkszeug der Führung**[978] ist.

977 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, S. 247, Kapitel 2 (Instrumente und Verfahren der Unternehmensentwicklung).

978 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, S. 249, Kapitel 2 (Instrumente und Verfahren der Unternehmensentwicklung).

Abbildung 18: Instrumente, Methoden und Verfahren der Unternehmensentwicklung[979]

979 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, S. 248, Abbildung 13.

Strategien und Konzepte sind nur so gut, wie sie von den betroffenen Menschen akzeptiert und umgesetzt werden. Ob und wie dies geschieht, hängt sehr stark von den Rahmenbedingungen im Arbeitsumfeld der Mitarbeiter ab. Das Umfeld kann Handeln erleichtern, aktiv unterstützen, erschweren oder nahezu unmöglich machen. Je stärker sich Mitarbeiter in ihren Erwartungen, Wertvorstellungen und Qualifikationen unterscheiden, desto weniger werden sie sich über einen Kamm scheren lassen, desto mehr lohnt es sich, sich mit den einzelnen Individuen zu beschäftigen, ihre persönlichen Voraussetzungen und Erwartungen kennen zu lernen[980]. Auf dieser Grundlage sollten die entsprechenden Maßnahmen entwickelt werden.

*2.8.11 Führen durch Zielvereinbarungen (**M**anagement **b**y **O**bjectives)*

Auch wenn intrinsische Motivation, also die Beschäftigung mit einer Sache um ihrer selbst willen, den Königsweg bildet, so ist das Erreichen eines lohnenswerten Ziels auch ein wichtiger motivationaler Baustein, der sowohl hilft die Startträgheit zu überwinden als auch die Ausdauer im Veränderungsprozess fördert.[981] Der Ansatz der »zielorientierten Führung« wird gerne auch dem **M**anagement **b**y **O**bjectives-Modell (**MbO**) zugeordnet. Doch kann er auch aus dem Verständnis des allgemeinen Führungsbegriffs abgeleitet werden, sofern man Führung als zielorientierte Gestaltung von Betrieben und Unternehmen bzw. Einflussnahme von Personen versteht.[982]

Zielvereinbarungen sind ein wesentlicher Bestandteil der Unternehmens- und Personalführung eines Unternehmens, um die gesteckten Unternehmensziele umzusetzen.[983] Bei Zielvereinbarungen treffen Vorgesetzte mit ihren Mitarbeitern oder ganzen Teams Abmachungen über anzustrebende Ziele.[984]

Ziele werden zwischen dem Mitarbeiter und dem Vorgesetzten in der Regel einmal pro Jahr im Rahmen eines sogenannten Zielvereinbarungsgespräches vereinbart und protokolliert. Das Protokoll wird im Anschluss von beiden gemeinsam unterschrieben.

---

980 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, S. 249.
981 *Lauer,* Change Management, 2. Aufl. 2014, S. 75, Abschnitt 5.6 Satz 1 (Erfolgsbaustein Zielmotivation).
982 *W. Simon,* Managementkonzepte von A bis Z, 2009, S. 549 Abschnitt 30. Zielorientiertes Führen Abs. 1.
983 *Wagner,* Strategie und Managementwerkzeuge, 2007, S. 110, Abschnitt 5.5 Zielvereinbarungen, Abs. 1 Satz 1.
984 Wirtschafts-Lexikon, 2006, S. 6385, Abschnitt I. Zielvereinbarung als Managementinstrument, Satz 1.

Eine Kopie erhält der Mitarbeiter, eine der Vorgesetzte und eine weitere Kopie erhält die Personalabteilung, welche dieses in der Personalakte ablegt.[985] Dabei ist zu beachten, dass es sich hierbei um brisante personenbezogene Daten handelt, die besondere Beachtung verlangt. In der Praxis hat sich das Ablegen auf einem verschlüsselten Laufwerk als Praktikabel herausgestellt. Sollten noch papierbasierende Personalakten geführt werden, so sind derartige Protokolle und Dokumente in einem verschlossenen bzw. versiegeltem Umschlag abzulegen und in einem verschlossenen Schrank aufbewahrt werden. Dadurch wird ein Zugriff für unbefugte zumindest erschwert.

Ziele sollen im Einzelnen sein:

S	**s**chriftlich fixiert, präzise und klar
M	**m**essbar, d.h. in Zahlen ausdrückbar, nachvollziehbar und überprüfbar
A	**a**nspruchsvoll, d.h. eine Herausforderung darstellend aber dennoch
R	**r**ealistisch und erreichbar
T	**t**erminiert, d.h. auf einen konkreten, festen Zeitraum bezogen

Abbildung 19: Anforderungen an Zielvereinbarungen nach der SMART-Regel

Es existieren unzählige Formulare zur Verwendung von Zielvereinbarungen. Aus der praktischen Erfahrung werden diese für die entsprechenden Abteilungen erstellt, angepasst und verwendet.

Die Beurteilung der Leistungen eines Mitarbeiters ist ein wichtiges, aber bei den Führungskräften auch ein wenig geliebtes Führungsinstrument. Oft erwarten Mitarbeiter eine jährliche Höherstufung. Die gängigen Punktebewertungen werden untereinander ausgetauscht und alle glauben, dass sie unterbewertet sind. Es gibt Frust und Ärger und man erreicht damit das Gegenteil von dem, was eigentlich bewirkt werden sollte, nämlich die Motivation der Mitarbeiter.[986]

985 *Wagner,* Strategie und Managementwerkzeuge, 2007, S. 110, Abschnitt 5.5 Zielvereinbarungen (jährliches Zielvereinbarungsgespräch).

986 *Wagner,* Strategie und Managementwerkzeuge, 2007, S. 112, Abschnitt 5.6 Leistungsbeurteilung.

In der Praxis hat sich häufig gezeigt, dass eine weniger positive Beurteilung, welche im Übrigen gemeinsam erstellt wurde und auf nachvollziehbaren Zielen ausgerichtet sein sollte, zur Unzufriedenheit geführt hat. In einzelnen Fällen führte dieses zur inneren Kündigung und in der Folge zur Trennung.

Besser ist eine Beurteilung des Mitarbeiters nach dem System der Zielvereinbarung und damit verbunden ein klares, nachvollziehbares Punkte - Bewertungssystem. Das Verfahren ist flexibel und die Beurteilungskriterien werden gemeinsam festgelegt und individuell abgestimmt. Dabei sind Skalierungen zu empfehlen, um eine schwarz-weiße Beurteilung auszuschließen.[987]

2.8.12 Prozessorientiertes Projektmanagement

Prozessorientiertes Projektmanagement unterscheidet sich in wesentlichen Punkten von konventionellen technokratischen Modellen. Der Hauptunterschied liegt in der ganzheitlichen Betrachtungs- und Vorgehensweise oder, anders ausgedrückt, im Berücksichtigen der strategischen und politischen Dimension von Projektarbeit.[988] Der Duden erklärt den Prozess wie folgt: „*über eine gewisse Zeit sich erstreckender Vorgang, bei dem etwas entsteht oder abläuft*“[989]. Nun würde diese Erläuterung nicht den Kern des Prozessorientierten Projektmanagements erfassen, aber grundsätzlich stimmt die Aussage. Diese müsste allerdings im Detail erfasst und um die entsprechenden Prozesse erweitert werden.

Changemanagement und Projektmanagement sind untrennbar miteinander verbundene Gebiete, da Wandel in aller Regel in Form von Projekten organisiert wird und das Projekt in gewissem Sinne als Organisationsform für wandlungsfähige Unternehmen schlechthin steht.[990]

Im Projektmanagement wird der Lösungsweg in verschiedene Teilschritte aufgeteilt.[991] Ein Projektleiter, der glaubt, es genüge, methodisch »sauber« vorzugehen, um ein großes, komplexes Projekt zum Erfolg zu führen, handelt blauäugig und verschleudert letztlich

---

987 *Wagner,* Strategie und Managementwerkzeuge, 2007, S. 113, Vergütungssystem Abs. 1.
988 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, S. 338, Kapitel 7, Prozessoriertes Projektmanagement.
989 *Dudenredaktion,* Das Bedeutungswörterbuch, 5. Aufl. 2018, S. 762.
990 *Lauer,* Change Management, 2. Aufl. 2014, S. 187, Abschnitt 12.1 Begriff und Erfolgsbeitrag.
991 *Meier,* Projektmanagement, 2007, S. 14, Abschnitt 3 Projektmanagement, Abs. 1 Satz 1.

in gewaltigem Umfang kostbare Ressourcen seines Unternehmens. Zwei Aspekte, über die herkömmliche Handbücher sich von vornherein ausschweigen, entscheiden nämlich weitgehend über den Verlauf der Projektarbeit: die Dynamik und die Vernetzungen.

- **Energie**: Wo liegt die »ownership« – wer betrachtet dieses Projekt als »seine Sache«? Wer alles ist am Erfolg des Projekts interessiert und bereit, sich persönlich dafür zu engagieren?
- **Macht**: Wer hat welchen Einfluss auf das Geschehen? Welches sind die »Schlüssel-Hierarchen«, welches die informellen »Opinion Leaders« – und wie können sie gewonnen werden?
- **Kräftefeld**: Was gibt es insgesamt für unterstützende, was für hindernde Einflüsse – und welche Konsequenzen ergeben sich aus diesem Kräftefeld für die Umsetzbarkeit von Maßnahmen?
- **Vernetzungen**: In was für ein Umfeld ist das Projekt eingebettet? Wer muss bei welchen Fragen aktiv einbezogen werden? Was für Informations- und Kommunikationskanäle müssen etabliert werden, damit eine reibungsarme Projektarbeit sichergestellt werden kann?[992]

Ein Projekt wird aus unterschiedlichsten Gründen lanciert. Nachfolgend sind die häufigsten Punkte, die zu einem Projektstart führen, aufgelistet:

- Optimierung der Arbeitsabläufe,
- Quantitative und qualitative Verbesserungen,
- Kundennähe
- Einsparungen,
- Steigerung der Wettbewerbs- und Leistungsfähigkeit,
- Gesetzliche, ökonomische oder ökologische Vorschriften und Vorgaben.[993]

2.8.13 Gestaltung der Kommunikation

Kommunikation soll alle Formen der interpersonellen Übermittlung von Informationen bzw. Botschaften im Rahmen von Change-Prozessen umfassen.[994] Kommunikation ist, so gesehen, der Weg, über den im ständigen Spiel von Informationen, Mitteilungen und

992 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, S. 338, Kapitel 7.
993 *Meier,* Projektmanagement, 2007, S. 21, Gründe für einen Projektstart.
994 *Lauer,* Change Management, 2. Aufl. 2014, S. 122, Abschnitt 8.1.1 Begriff.

Verstehen Menschen gemeinsam Sinn erzeugen.[995] Tief greifender Wandel ist normalerweise unmöglich, wenn nicht alle Mitarbeiter gewillt sind, zu unterstützen, oftmals auch durch kurzfristige Opfer. Auch wenn Menschen mit dem Status quo unzufrieden sind, werden sie keine Opfer bringen, solange sie nicht davon überzeugt sind, dass die Vorteile des Wandels überwiegen und die Transformation auch tatsächlich durchführbar ist. Ohne eine intensive und glaubwürdige Kommunikation werden Herz und Verstand der Mitarbeiter nicht für die Sache gewonnen.[996]

Kommunikation kann als eine Art Katalysator des Change-Managements bezeichnet werden. Sie allein reicht nicht aus, um Wandel erfolgreich zu managen, aber ohne sie kann Wandel weder initiiert noch durchgeführt werden. Als Katalysator des Wandels erfüllt sie dabei insbesondere folgende Aufgaben[997]:

- Schaffung von informatorischer Transparenz
- Erkennen und Abschwächen von Widerstand
- Verstärkung des Prozesses im Sinne positiver Rückkopplung
- Förderung der sozialen Integration[998]

Die Themen sind ausgewählt und klare Schwerpunkte gesetzt. Innerhalb des Kommunikationskonzepts beschäftigen sich Themenplanung vorrangig mit den Schwerpunktthemen.[999]

Zu dem Zweck steht eine Reihe von Techniken zur Verfügung, die helfen die Themen interessant aufzubereiten, ins Gespräch zu bringen und über längere Zeit dort zu halten.[1000]

---

995 *Plate,* Grundlagen der Kommunikation, 2. Aufl. 2015, S. 10.
996 *Kotter,* Leading change, 2015, S. 7, Kapitel 1, Warum Unternehmen scheitern.
997 *Lauer,* Change Management, 2. Aufl. 2014, S. 124, Abschnitt 8.1.2 Erfolgsbeitrag.
998 *Lauer,* Change Management, 2. Aufl. 2014, S. 124, Abschnitt 8.1.2 Erfolgsbeitrag.
999 *Schmidbauer/Jorzik,* Wirksame Kommunikation – mit Konzept, 2017, S. 309, Themen inhaltlich aufbereiten, Satz 1 und Satz 2.
1000 *Schmidbauer/Jorzik,* Wirksame Kommunikation – mit Konzept, 2017, S. 310 Abs. 3.

- **Themen fokussieren**
  Wir fokussieren Themen indem wir einen bestimmten Themenaspekt besonders hervorheben.
- **Themen aktualisieren**
  Themen entwickeln sich weiter, wir beobachten die Entwicklung und berichten über die Fortschritte.
- **Themen extrapolieren**
  Themen, die bereits laufen, werden extrapoliert, d.h., auf die Folgen hin überprüft.
- **Themen lokalisieren**
  Themen werden geografisch zugeordnet.
- **Themen illustrieren**
  Themen werden mit Fotos, Videoclips oder Grafiken illustriert, um so komplexe Sachverhalte anschaulich zu machen.
- **Themen kombinieren**
  Zwei Themen erzielen in der Kombination einen stärkeren Neuigkeitswert und eröffnen ungeahnte Perspektiven.
- **Themen kontrapunktieren**
  Ein Thema wird gegenläufig zum Mainstream entwickelt und gewinnt dadurch mehr Aufmerksamkeit.
- **Themen personalisieren**
  Das Thema wird anhand eines handelnden Protagonisten dargestellt.
- **Themen interpretieren**
  Es werden keine neuen Themeninhalte vorgestellt, sondern die vorhandenen Fakten neu und anders aufbereitet.[1001]

Kommunikation äußert sich sowohl in Worten als auch in Taten. Letztere sind generell die wirkungsvollere Form. Nichts untergräbt den Wandel mehr als ein im Widerspruch zu den Inhalten der verbalen Kommunikation stehendes Verhalten der Schlüsselspieler.[1002]

1001 *Schmidbauer/Jorzik,* Wirksame Kommunikation – mit Konzept, 2017, S. 310 und 311.
1002 *Kotter,* Leading change, 2015, S. 8, Teil I.

2.8.14 Konfliktmanagement

Konflikte sind an sich eine ganz normale und alltägliche Begleiterscheinung menschlichen Zusammenlebens. Es gibt keine dauerhaft konfliktfreien Beziehungen. Wo immer Menschen zusammenwirken, treffen unterschiedliche Meinungen, Bedürfnisse und Interessen aufeinander – mal zwischen einzelnen Individuen, mal zwischen kleineren Gruppen, mal auch zwischen großen Organisationen. Und wenn irgendwo irgendwelche Veränderungen anstehen, sind Konflikte von vornherein programmiert – denn da gibt es immer die einen, die etwas Neues schaffen wollen, und die anderen, die den bisherigen Zustand erhalten möchten. Es gibt keine Veränderung ohne Konflikt.[1003]

Die Kunst besteht darin, einen Konflikt nicht eskalieren zu lassen und die betroffenen Parteien frühzeitig „einzufangen" bevor die Fronten verhärten. Sobald eine Seite glaubt, von der anderen nicht ernst genommen, in ihrer Würde und Integrität verletzt oder gar vorsätzlich angelogen oder missbraucht zu werden, reagiert sie mit Wut und Empörung.[1004]

Jeder Konflikt hat seine Geschichte. Er ist nicht irgendein plötzliches und schon gar kein zufälliges Ereignis, sondern das Ergebnis eines ganz bestimmten Entwicklungsprozesses. Ein Konflikt wird »gelernt« – und wer ihn aus der Welt schaffen will, muss dafür sorgen, dass er wieder »verlernt« wird. Verständnis für das Geschehene muss gewonnen, Misstrauen schrittweise abgebaut, Vertrauen schrittweise wiederaufgebaut werden. Der Weg, der in die Irre geführt hat, muss **gemeinsam** ein Stück weit zurückgegangen werden, bevor man ohne Gefahr eines Rückfalls gemeinsam einen neuen Weg in die Zukunft gehen kann.[1005]

1003 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, S. 455.
1004 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, S. 457, Abschnitt 3, Eskalation.
1005 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, S. 459, Grundvoraussetzungen für eine Konfliktregulierung.

Nachfolgende Abbildung stellt das „Konfliktmanagement“ grafisch dar und verdeutlicht in der Folge die Verknüpfungen und die Wichtigkeit der einzelnen Bereiche.

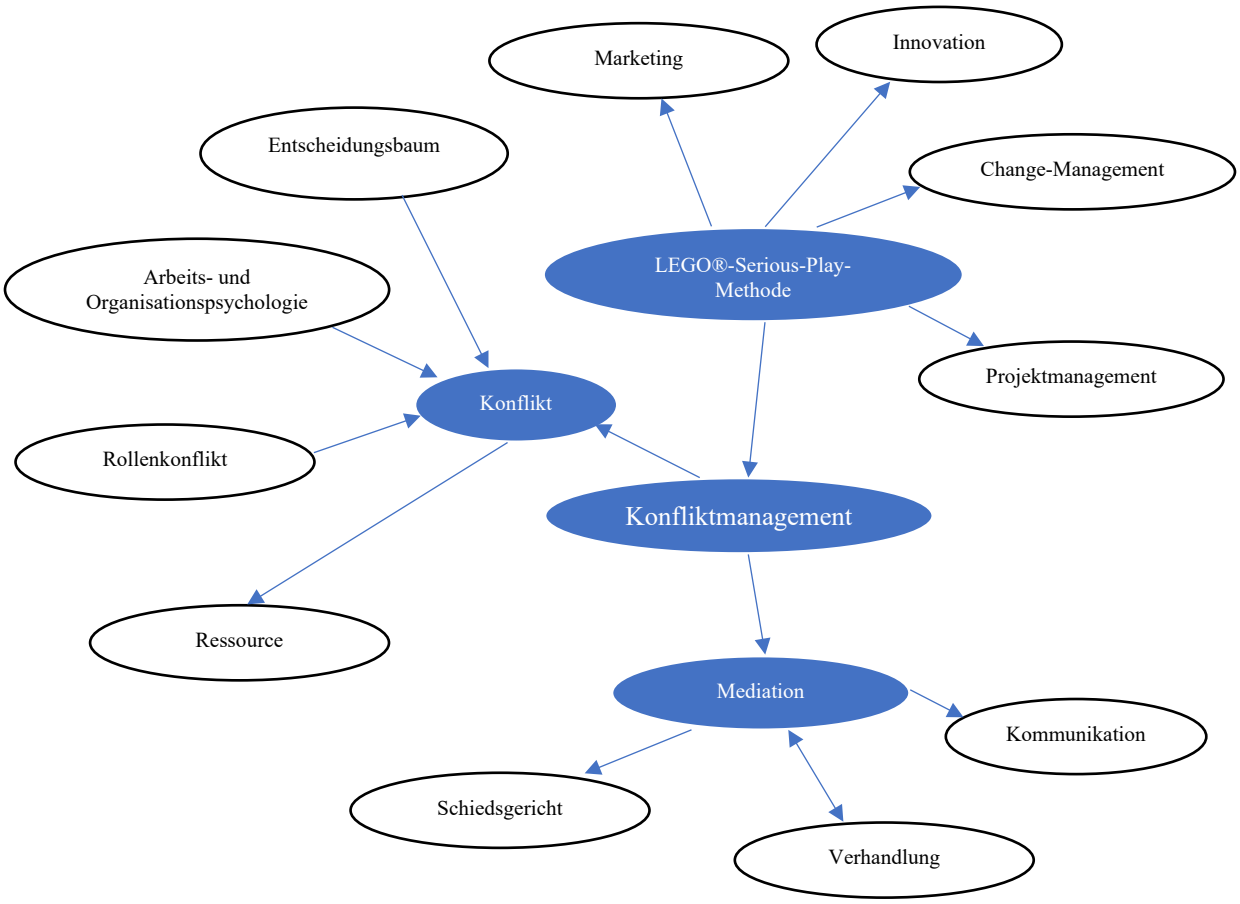

Abbildung 20: Konfliktmanagement[1006]

1006 *Springer Gabler Verlag* (Hrsg.), Konfliktmanagement, Feststellung, Steuerung und Regelung von Konflikten durch spezifische Handhabungsformen, etwa Verhandlung, Vermittlung, Schlichtung einschließlich Zwangsschlichtung., https://wirtschaftslexikon.gabler.de/definition/konfliktmanagement-41409/version-264774.

2.8.15 Geschäftsprozessoptimierung

Die meisten Unternehmen sind immer mal wieder mit zwei Problemen konfrontiert: zu hohe Kosten und schwindende Erträge. Weltunternehmen solidester Art, von denen man noch vor wenigen Jahren gesagt hätte, ihr Wohlstand sei Naturgesetz, geraten ins Trudeln und sehen sich zu tiefgreifenden Restrukturierungen gezwungen. Unternehmen, die zu lange nicht an die Zukunft gedacht haben, verschwinden ganz einfach von der Bildfläche. Aber auch gesunde und grundsätzlich erfolgreiche Unternehmen müssen Kosten und Erträge optimieren, um überleben zu können.[1007]

Business Reengineering und Geschäftsprozessoptimierung sind, obgleich die Begriffe nicht selten synonym verwendet werden, unterschiedliche Ansätze zur Restrukturierung der Geschäftsprozesse eines Unternehmens. Die Zielsetzung der Geschäftsprozessoptimierung ist die nachhaltige Verbesserung der Wettbewerbsfähigkeit eines Unternehmens durch Ausrichtung aller wesentlichen Arbeitsabläufe an den Kundenanforderungen. Dies bedeutet vor allem eine Fokussierung der Bemühungen auf diejenigen Geschäftsprozesse, die direkt durch Kundenaktionen (z.B.: Bestellung, Zahlung einer Rechnung, Reklamation) ausgelöst werden.[1008]

Wesentliche Ziele der Geschäftsprozessoptimierung sind die Verkürzung der Durchlaufzeit und die Verbesserung der Prozessqualität. Die nachfolgende Tabelle stellt grundsätzliche Gestaltungsmöglichkeiten dar.

1007 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, S. 520, Kapitel 15 Ergebnisverbesserung durch Geschäftsoptimierung, Abs. 1.

1008 *Gadatsch,* Grundkurs Geschäftsprozess-Management, 9. Aufl. 2020, Position 1272 von 4179, Abschnitt 2.4.2 Geschäftsprozessoptimierung, Abs. 1.

Nr.	Konzept	Erläuterung
1	Weglassen	Überprüfung der Notwendigkeit von Prozessen oder Teilprozessen zur Funktionserfüllung, Abschaffung von Medienbrüchen, Abschaffung von nicht sinnvollen Genehmigungsschritten
2	Auslagern	Vergabe von Teilprozessen oder vollständigen Prozessketten durch externe spezialisierte Dienstleister (z.B. Buchführung und Bilanzierung durch einen Steuerberater)
3	Zusammenfassen	Arbeitsteilige Aufgaben werden so zusammengefasst, dass ein Bearbeiter zusammengehörige Teilprozesse vollständig ohne Bearbeiterwechsel durchführt (z.B. Kundenberatung und Auftragserfassung bis zur Erstellung der Auftragsbestätigung)
4	Parallelisieren	Erhöhung der Arbeitsteilung bei parallelisierbaren Teilschritten (z.B. Klausurkorrektur durch mehrere Prüfer je Teilgebiet)
5	Verlagern	Verlagerung von Prozessschritten, so dass Aufgaben frühzeitig durchgeführt werden, ohne später zu einem Flaschenhals zu werden (z.B. vollständige Erfassung der Kundeninformationen bei Auftragserfassung)
6	Beschleunigen	Einsatz von zeitsparenden Arbeitsmitteln (Dokumentenmanagementsystem ersetzt Papierdokumentation), Reduzierung von Warte- und Liegezeiten durch Erhöhung von Kapazitäten
7	Schleifen vermeiden	Schleifenfreie Gestaltung von Prozessen, d.h. Verzicht auf Wiederholung von Teilschritten eines Prozesses (z.B. Onlineerfassung aller Kunden- und Bestelldaten im Rahmen der Auftragserfassung und Freigabe des Auftrages erst nach vollständiger Plausibilisierung der Daten)
8	Ergänzen	Vermeidung von nachgelagerten Prozessen zur „Schadensbeseitigung“ (z.B. Ergänzung einer Qualitätskontrolle nach der Teilemontage um einen möglichen „Nachbearbeitungsprozess“ oder eine „Rückholaktion fehlerhafter Ware“ zu vermeiden).

Abbildung 21: Tabelle in Anlehnung an Bleicher (1991), Inhalt aus Gadatsch 2020[1009]

1009 *Gadatsch,* Grundkurs Geschäftsprozess-Management, 9. Aufl. 2020, Position 1283 von 4179, Tabelle . 2.1 „modifiziert“.

Die häufigsten und gleichzeitig gröbsten Fehler, die in der Praxis begangen werden können, im Besonderen wenn Kostenstrukturanalysen und Kostensenkungsmaßnahmen auf dem Programm stehen, werden seitens Doppler/Lauterburg (2014) als die „sieben Todsünden“ bezeichnet.

1. Lineare Kürzungen
2. Einseitige Sparoptik
3. Unrealistische Vorgaben
4. Aussteuern der Linienverantwortung
5. Tabuisieren der Hierarchie
6. Übergehen wichtiger Partner
7. Mangelnde Umsetzung[1010]

Es gibt in der Praxis die verschiedensten Ansätze, um die Ergebnisse zu verbessern – von einfallslosen Sparübungen über systematische Kostensenkungsprogramme und Ertragspotenzialermittlungen bis hin zu strategisch angelegten Konzepten wie etwa die Zertifizierung nach ISO 2000, der so genannte **K**ontinuierliche **V**erbesserungs**p**rozess (**KVP**), **T**otal **Q**uality **M**anagement (**TQM**) oder **Kaizen** (**KAI** = kontinuierliche Veränderung, **ZEN** = zum Besseren). Der mit Abstand wirksamste, gleichzeitig, aber auch anspruchsvollste Ansatz ist die **G**eschäfts**p**rozess**o**ptimierung (**GPO**). Im Gegensatz zu einem weitverbreiteten Missverständnis geht es nicht darum, die Abläufe im Rahmen der bestehenden Organisation zu optimieren, sondern darum, die Art und Weise, wie das Geschäft betrieben beziehungsweise der Markt bearbeitet wird, grundlegend neu zu gestalten.[1011]

1010 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, S. 521 f. (sieben Todsünden).
1011 *Doppler/Lauterburg,* Change Management, 13. Aufl. 2014, S. 531, Geschäftsprozessoptimierung.

Nachfolgende Grafik zeigt die Vorgehensweise bei der Optimierung und Verbesserung der jeweiligen Prozesse auf. Es handelt sich hierbei lediglich um eine grobe Darstellung. Die Umsetzung hat entsprechend der Unternehmensstruktur und den betroffenen Abteilungen detaillierter zu erfolgen.

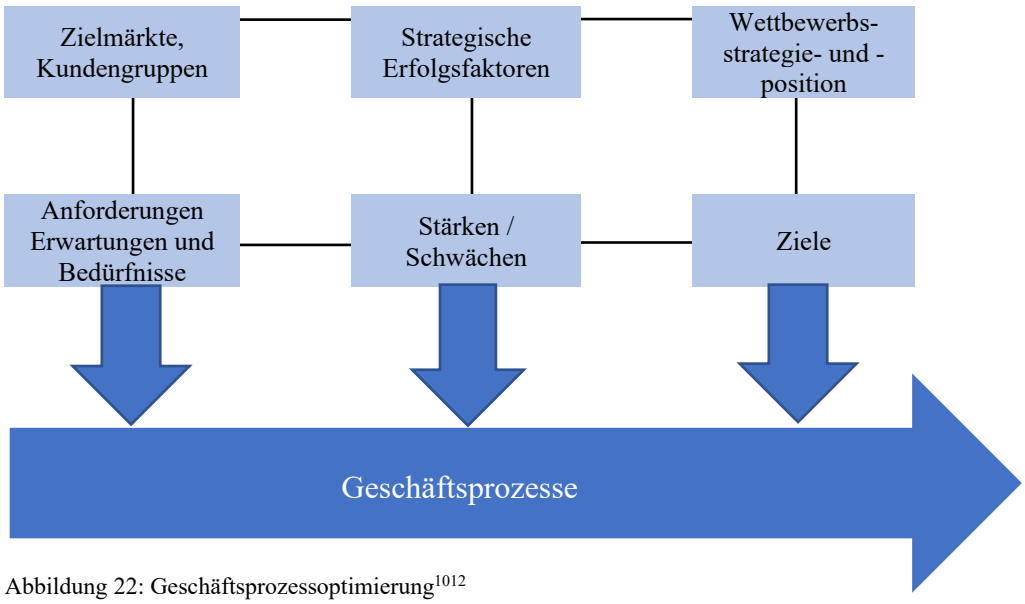

Abbildung 22: Geschäftsprozessoptimierung[1012]

1012 *Schmelzer/Sesselmann,* Geschäftsprozessmanagement in der Praxis, 7. Aufl. 2010, S. 123.

2.9 Datenschutz durch Technikgestaltung (Art. 25, 32 DS-GVO)

Die in Art. 25 geregelten Vorgaben werden (auch im deutschsprachigen Raum) häufig unter den Schlagworten **Privacy by Design** bzw. **Privacy by Default** diskutiert. Das ist nicht präzise und hat letztlich historische Gründe. Privacy by Design als neues, proaktives Konzept, bei dem die Technik in den Dienst der Rechtsdurchsetzung gestellt wird…[1013]

Die Datenschutz-Grundverordnung (DS-GVO) setzt neue Maßstäbe für die IT-Sicherheit im Bereich des Datenschutzes.[1014] Durch Art. 25 werden spezifische Verpflichtungen der Verantwortlichen zum Schutz personenbezogener Daten geschaffen, die es in dieser Form im deutschen Datenschutzrecht bisher noch nicht gab.[1015] Es handelt sich um ein, jedenfalls auf europarechtlicher Ebene, weitgehend neues Konzept, auch wenn Privacy by Design, in reduziertem Kontext häufig unter dem Stichwort **P**rivacy **E**nhanding **T**echniques (**PET**) genannt, im Grunde bis in die Anfänge der datenschutzrechtlichen Gesetzgebung zurückverfolgt werden kann.[1016]

2.9.1 Privacy by Design (Art. 25 Abs. 1 DS-GVO)

Wie dargestellt, greift die Formulierung von Art. 25 Abs. 1 die Grundprinzipien des Privacy by Design nicht unmittelbar bzw. vollständig auf, sondern formuliert lediglich Voraussetzungen und Ziele und lässt die konkreten Maßnahmen, mit Ausnahme von Beispielen, weitgehend abstrakt. Dementsprechend wird es wesentlich auf die Auslegung der Anforderungen des Art. 25 ankommen.

Ziel ist nach Art. 25 Abs. 1 die Einhaltung der datenschutzrechtlichen Grundsätze des Art. 5 Abs. 1, beispielhaft ist im Gesetzestext die ***Datenminimierung*** genannt.[1017] Die Pflicht des Verantwortlichen aus Art. 25 Abs. 1 ist es, angemessene technisch-organisatorische Maßnahmen zu treffen.[1018] Art. 25 Abs. 1 spricht von geeigneten

---

1013 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Art. 25 Allgemein, Rn. 19, Position 30830 von 87533.

1014 *Karsten U. Bartels LL.M., Merlin Backer LL.M.*, Die Berücksichtigung des Stands der Technik in der DSGVO, Neue Anforderungen an die IT-Sicherheit im Datenschutz, in Datenschutz Datensich, 214 f.

1015 *Däubler et al.,* EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, S. 363, Rn. 1 Satz 1.

1016 *Sydow u. a.* (Hrsg.), Europäische Datenschutzgrundverordnung, Mantz, S. 606, Rn. 1, Art. 25 DSGVO.

1017 *Bäcker,* Datenschutz-Grundverordnung, Hartung, S. 509, Rn. 14, Art. 25 Abs. 1 DSGVO.

1018 *Bäcker,* Datenschutz-Grundverordnung, Hartung, S. 509, Rn. 15 Satz 1, Art. 25 Abs. 1 DSGVO.

technisch-**o**rganisatorischen **M**aßnahmen (**TOM**) und greift damit eine Begrifflichkeit auf, die auch in Art. 24, 28 und 32 Verwendung findet; im Rahmen des Art. 25 aber im Lichte seines spezifischen (zeitlich vorwirkenden) Ziels gesehen werden muss, Technik von Anfang an so zu entwickeln, dass sie nur datenschutzfreundlich arbeiten kann.[1019] Auch „zum Zeitpunkt der eigentlichen Verarbeitung" muss der Verantwortliche nach dem Willen des Gesetzgebers geeignete technische und organisatorische Maßnahmen ergreifen. Er steht damit während der gesamten Verarbeitungskette der Daten in der Verantwortung, seine geplanten Maßnahmen im Einklang mit den Geboten der DS-GVO umzusetzen, sie insbesondere auch möglichen neuen Erkenntnissen anzupassen.[1020]

2.9.2 Stand der Technik

Wie bereits nationale Gesetze zur IT-Sicherheit und zum technischen Datenschutz, enthält auch sie den Verweisungsbegriff „Stand der Technik" als ein wesentliches Merkmal für die Feststellung des jeweiligen Schutzniveaus technischer und organisatorischer Maßnahmen.[1021]

Art. 25 Abs. 1 Satz 1 DS-GVO, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, „Unter Berücksichtigung des Stands der Technik…"[1022]

Der Begriff, „Stand der Technik" ist zwar auch an anderen Stellen der DS-GVO wie in Art. 32 Abs. 1 Satz 2 DS-GVO zu finden, wird aber in der Verordnung nicht definiert.[1023]

Schwierigkeiten bereitet der Begriff des „Stand der Technik" im Sinne des Art. 25 Abs. 1, da die DS-GVO, wie dies auch schon bei der Vorgabe zur Verarbeitungssicherheit in Art. 17 der Datenschutzrichtlinie 95/46[1024] der Fall war, für die Interpretation dieses unbestimmten Rechtsbegriffs wenig Anhaltspunkte liefert. In der englischen Sprachfassung ist in Art. 25 Abs. 1 von „*state of the art*", in der französischen

---

1019 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 30944 von 87533, Rn. 31, Art. 25 Abs. 1 DSGVO.

1020 *Ehmann/Selmayr/Albrecht* (Hrsg.), DS-GVO, Martini, S. 333, Rn. 43c, Art. 25 Abs. 1 DSGVO.

1021 *Karsten U. Bartels LL.M., Merlin Backer LL.M.*, Die Berücksichtigung des Stands der Technik in der DSGVO, Neue Anforderungen an die IT-Sicherheit im Datenschutz, in Datenschutz Datensich, 214 f.

1022 Datenschutz Grundverordnung vom 27.04.2016, Art. 25 Abs. 1 Satz 1 DSGVO.

1023 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, S. 613, Rn. 46, Art. 25 DSGVO.

1024 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates.

Sprachfassung von „*l'état des connaissances*“ und in der spanischen Sprachfassung von „*el estado de la técnica*“ die Rede. Das ist insoweit bemerkenswert, als die deutsche und englische Sprachfassung im Rahmen der DS-GVO begrifflich bei der Terminologie der Datenschutzrichtlinie bleiben („ Stand der Technik“, „state of the art“), während die spanische und französische Sprachfassung eine gegenüber der Formulierung in der Datenschutzrichtlinie abweichende Begrifflichkeit verwenden.[1025] Rechtssystematisch ist der Stand der Technik ein Verweisungsbegriff. Er gibt einer objektiv-technischen Information durch die Bezugnahme auf ein gesetzliches Schutzziel eine rechtliche Bedeutung.[1026]

Zunächst gilt es zu beachten, dass der Begriff im Rahmen der DS-GVO autonom auszulegen ist. Ein Rückgriff auf deutsche Gesetze (wie etwas das BSIG[1027]) oder nationale Rechtsprechung zu entsprechenden Vorschriften, ist nicht möglich.[1028]

„Stand der Technik“ bewegt sich in seinem Anforderungsprofil zwischen „**allgemein anerkannten Regeln der Technik**“ einerseits und „**Stand der Wissenschaft und Technik**“ anderseits.[1029] Anders als den „allgemein anerkannten Regeln der Technik“, verlangt diese die Bewährung der Techniken in der Praxis und ihre Anerkennung durch die überwiegende Zahl der Fachleute. „Stand der Technik“ geht darüber hinaus: Das Groß der Fachleute meint solche Verfahren, die einem fortgeschrittenen Stand der technischen Entwicklung entsprechen.[1030] Anders als dem **Stand der Wissenschaft und Technik** kommt es dem **Stand der Technik** darauf an, dass die Verfahren technisch tatsächlich realisierbar sind. Er beschreibt also Maßnahmen, die dem aktuell technisch Möglichen

1025 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Art. 25 Abs. 1 Satz 1 DSGVO, Position 31076 von 87533, Rn. 44.

1026 *Karsten U. Bartels LL.M., Merlin Backer LL.M.*, Die Berücksichtigung des Stands der Technik in der DSGVO, Neue Anforderungen an die IT-Sicherheit im Datenschutz, in Datenschutz Datensich, 214 f.

1027 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik.

1028 *Gola u. a.* (Hrsg.), Datenschutz-Grundverordnung, S. 481, Rn. 15, Art. 32 DSGVO.

1029 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Martini, S. 331, Rn. 39a, Art. 25 DSGVO.

1030 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Martini, S. 331, Rn. 39c, Art. 25 DSGVO.

entsprechen, auf gesicherten Erkenntnissen der Wissenschaft und Technik beruhen und in ausreichendem Maße zur Verfügung stehen.[1031] [1032]

So geht aus Erwägungsgrund 78 hervor, dass die Regelung ausdrücklich für Hersteller von Produkten oder Anbieter von Diensten als Appell dergestalt zu gelten hat, dass diese ermutigt werden, datenschutzfreundliche Produkte, Systeme und Dienste anzubieten und einzuführen.[1033]

Erwägungsgrund 78

Zum Schutz, der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by Design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die

1031 *Gola u. a.* (Hrsg.), Datenschutz-Grundverordnung, S. 481, Rn. 15 Art. 32 DSGVO.
1032 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Martini, S. 331, Rn. 39d.
1033 *Roßnagel/Barlag* (Hrsg.), Europäische Datenschutz-Grundverordnung, Barlag, § 3 Allgemeine Regeln der Datenschutz-Grundverordnung, Rn. 227.

Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden.[1034]

2.9.3 Privacy by Default (Art. 25 Abs. 2 DS-GVO)

In Art. 25 Abs. 2 werden die auch in Abs. 1 zu Tage tretenden Prinzipien nutzerseitiger Kontrolle und Transparenz abermals technisch adressiert, und noch einen Schritt weitergehend, speziell hinsichtlich ihrer jeweiligen Standardeinstellung auf Datenschutzfreundlichkeit vorprogrammiert.[1035] Damit wird erstens dem Umstand Rechnung getragen, dass es (auch unter dem Aspekt der Datensicherheit) ***einen* Unterschied macht, ob Daten nur nicht verwendet oder gar nicht erst erhoben werden**.[1036] Dies muss - und das ist das Neue an der Vorschrift- durch Voreinstellungen realisiert werden.[1037]

Nach Art. 25 Abs. 2 S. 1 hat der Verantwortliche geeignete TOMs zu ergreifen, um sicherzustellen, dass durch Voreinstellungen grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Ausgangspunkt ist demnach der datenschutzrechtliche Zweckbindungs- und Erforderlichkeitsgrundsatz (Art. 5 Abs. 1 lit. b und c). Nur diejenigen Datenarten, die für die jeweils konkret festgelegten Verarbeitungszwecke (Art. 30 Abs. 1 lit. b) erforderlich sind, sollen erhoben werden. Mit dem in Art. 25 Abs. 2 S. 1 so nur in der deutschen Sprachfassung auftauchenden Adjektiv „grundsätzlich“ könnte eine Einschränkung verbunden sein. Wie ein Vergleich mit anderen Sprachfassungen zeigt, lassen sich damit Ausnahmen aber nicht begründen.[1038] [1039]

1034 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 78 DSGVO.

1035 *Wybitul* (Hrsg.), EU-Datenschutz-Grundverordnung, S. 396, Kapitel IV, Art. 25 Abs. 2 DSGVO.

1036 *Schantz/Wolff,* Das neue Datenschutzrecht, 2017, Rn. 838.

1037 *Däubler et al.,* EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, S. 371, Rn. 41, Art. 25 Abs. 2 DSGVO.

1038 *Felix Bieker/Marit Hansen* RDV / Recht der Datenverarbeitung Heft 4, 165 f.

1039 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Rn. 61, Position 31236 von 87533, Art. 25 Abs. 2 Satz 1 DSGVO.

Datenverarbeiter verspüren den Anreiz, einem Dienstnutzer in möglichst reichem Umfang personenbezogene Daten abzuringen, bilden diese als Rohstoff des 21. Jahrhunderts doch die sprudelnde Quelle ihres wirtschaftlichen Ertrages.[1040]

Art. 25 Abs. 2 S. 2 konkretisiert weiter dahingehend, dass sich die Erforderlichkeit auf die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit bezieht. Der Umfang bezeichnet dabei (in Abgrenzung zur reinen Menge der Daten) die Tiefe der Verarbeitung, beispielsweise durch Erstellung von Persönlichkeitsprofilen.[1041] Da der Verantwortliche den Verarbeitungszweck festlegt, entscheidet er zugleich über den Umfang der dafür erforderlichen Daten. Die Speicherfrist für personenbezogene Daten muss nach Erwägungsgrund 39 auf das unbedingt erforderliche Mindestmaß beschränkt bleiben. Im Zuge dessen hat der Verantwortliche Fristen für ihre Löschung vorzusehen (sog. Löschkonzept).[1042]

Erwägungsgrund 39

… die personenbezogenen Daten sollten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen. Es sollten alle vertretbaren Schritte unternommen werden, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden. Personenbezogene Daten sollten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben

1040 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Martini, S. 333, Rn. 45, Satz 1, Art. 25 Abs. 2 Satz 1 DSGVO.

1041 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Martini, S. 335, Rn. 50, Art. 25 Abs. 2 Satz 1 DSGVO.

1042 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Rn. 62, Position 31236 von 87533, Art. 25 Abs. 2 DSGVO.

und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.

2.9.4 Cookies

Wie bereits in Teil 1 dargestellt, handelt es sich bei Cookies um kleine Textprogramme, welche den Besuch einer Webseite auf dem jeweiligen Rechner abspeichern. Cookies werden aktuell unter anderem für die personalisierte Werbung eingesetzt, um eine zielgerichtete Werbung projizieren zu können. Das heißt, Cookies haben die Aufgabe, den Nutzer „wieder zu erkennen", d.h. wer hat sich mit welchem Nutzernamen an welchem Tag auf welche Seite begeben und was hat dieser sich dort angesehen oder welche Produkte wurden angeklickt. Dadurch werden bei einem Besuch einer anderen oder derselben Seite dieselben Produkte und oder Produktlinie angezeigt, bzw. beworben.

Der Einsatz von Cookies wird durch die Programmierer der jeweiligen Webseite als Quellcode einprogrammiert und bei Aufruf der entsprechenden Seite durch ein Pop-Up Fenster aktiviert. In vielen Mitgliedstaaten der Europäischen Union ist seit der Anpassung der ePrivacy-Richtlinie (2002/58/EG) durch die als Cookie-Richtlinie bekannte Richtlinie 2009/136/EG ein **Opt-In** aber auch für andere vergleichbare Tracking-Technologien zwingend vorgesehen. In Deutschland wurde Art. 5 Abs. 3 der ePrivacy-Richtlinie trotz anderer Äußerungen bislang nicht umgesetzt, sondern weiterhin § 15 Abs. 3 S. 1 TMG angewendet, der bei einer pseudonymen Verarbeitungstätigkeiten eine **Opt-Out-Lösung** für das Erstellen von Nutzerprofilen und das Setzen hierfür erforderlicher Cookies oder Tracking-Pixel genügen lässt.[1043]

Die Suchmaschinenbetreiber benutzen Cookies (gewöhnlich dauerhafte Cookies) zur Verbesserung der Qualität ihrer Dienstleistungen, indem sie die Benutzereinstellungen speichern und typische Merkmale des Benutzers, etwa sein Suchverhalten, verfolgen. Die meisten Browser **waren** standardmäßig so konfiguriert, dass sie Cookies akzeptieren. Der Browser kann aber auch so eingestellt werden, dass er alle Cookies ablehnt, nur Sitzungs-Cookies akzeptiert oder anzeigt, wann ein Cookie übermittelt wird. Eventuell

1043 *Laue/Kremer,* Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl. 2019, Kremer, S. 97, Rn. 12.

funktionieren manche Merkmale und Dienste jedoch nicht richtig, wenn Cookies grundsätzlich abgelehnt werden.[1044]

In der Regel lässt der Datensatz eines Cookies keinen Personenbezug zu. Hat der Nutzer aber bei den Cookie ablegenden Anbieter zu einem früheren Zeitpunkt Identifikationsmerkmale (z.B. seine IP-Adresse) hinterlassen oder hinterlässt er solche zu einem späteren Zeitpunkt (Bspw. im Rahmen eines Bestell- oder Registrierungsvorgangs), kann die Information des Cookie-Datensatzes den Identifikationsmerkmalen des Nutzers zugeordnet werden. Möglich ist die Herstellung eines Personenbezugs ebenfalls, wenn der Nutzer mehrere Dienste desselben Anbieters nutzt (Google Mail, Google Chrome und Google Suchmaschine). In diesen Fällen kann der Anbieter den gebildeten Profilen meist sogar den Namen des Nutzers zuordnen.[1045]

Benutzer-Cookies werden von der Suchmaschine übermittelt und auf dem Computer des Benutzers gespeichert. Der Inhalt der Cookies kann je nach Suchmaschinenbetreiber unterschiedlich sein. Die von Suchmaschinen gesetzten Cookies enthalten typischerweise Informationen über das Betriebssystem und den Browser des Benutzers sowie eine eindeutige Identifikationsnummer für jedes Benutzerkonto. Sie ermöglichen eine genauere Identifizierung des Benutzers als die IP-Adresse. Wenn beispielsweise mehrere Benutzer mit jeweils eigenem Konto denselben Computer benutzen, würde jeder Benutzer ein eigenes Cookie erhalten, der ihn als Benutzer des Computers eindeutig identifiziert. Wenn ein Computer eine dynamische und variable IP-Adresse besitzt und die Cookies am Ende einer Sitzung nicht gelöscht werden, kann mit einem derartigen Cookie der Benutzer von einer IP-Adresse zur nächsten verfolgt werden. Das Cookie kann auch zur Korrelation von Suchvorgängen verwendet werden, die von nomadischen Computern wie beispielsweise Laptops gestartet werden, da ein Benutzer an verschiedenen Orten dasselbe Cookie hätte. Wenn sich mehrere Computer einen Internet-Anschluss teilen (z. B. hinter einer Box oder einem Router mit Adressübersetzung der

1044 *ARTIKEL-29-DATENSCHUTZGRUPPE,* Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, WP 148.

1045 *Bäcker,* Datenschutz-Grundverordnung, Klar/Kühling, S. 132, Rn. 36 - Vgl. hierzu ebenfalls Art.-29 Datenschutzgruppe WP 148, S. 24.

Absenderadresse (**N**etwork **A**ddress **T**ranslation – **NAT**), ermöglicht das Cookie die Identifizierung der einzelnen Benutzer an den verschiedenen Computern.[1046]

In Art. 95 der DS-GVO werden in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der EU keine zusätzlichen Pflichten auferlegt, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.[1047] Art. 95 dient der Begrenzung der DS-GVO auf das allgemeine Datenschutzrecht. Die Verordnung soll nicht übermäßig in das Feld der Telekommunikationsregulierung eingreifen.[1048]

Wegen der ausdrücklichen Ausnahmeregelung des Art. 95 DS-GVO ist für Erlaubnis zur Verarbeitung von Cookies allerdings nach wie vor die „ePrivacy-Richtlinie" 2002/58/EG in der durch die Cookie-Richtlinie 2009/136/EG geänderte Fassung maßgeblich mit den dies umsetzenden nationalen Gesetzen. Denn in der e-Privacy-Richtlinie ist die Verwendung von Cookies in Art. 5 Abs. 3 ausdrücklich geregelt und diese Regelung verfolgt dasselbe Ziel wie die DS-GVO, den Schutz der personenbezogenen Daten.[1049]

Die ePrivacy-Richtlinie enthält keine eigene Definition der Einwilligung, sondern verweist auf die mit der Datenschutz-Grundverordnung aufgehobene Datenschutz-Richtlinie (95/46/EG). Damit scheinen für die Anforderungen an die Einwilligung im Sinne des Art. 5 Abs. 3 der ePrivacy-Richtlinie gemäß Art. 94 Abs. 2 S. 1 nunmehr ebenso wie in Art. 6 Abs. 1 lit. a, Art. 9 Abs. 1 lit. a DS-GVO die Festlegung in Art. 7 und Art. 4 Nr. 11 relevant zu sein.[1050]

Erwägungsgrund 42 führt aus, dass die Verantwortlichen Vorkehrungen treffen sollten, um sicherzustellen, dass die betroffene Person weiß, worin sie eingewilligt hat. So sollen Einwilligungserklärungen von Unternehmen für betroffene Personen so klar und so

---

1046 *ARTIKEL-29-DATENSCHUTZGRUPPE,* Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, WP 148.

1047 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).

1048 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Heun/Assion, S. 1148, Rn. 2 zu Art. 95 DS-GVO.

1049 *Spindler/Schmitz/Liesching,* Telemediengesetz mit Netzwerkdurchsetzungsgesetz; Kommentar, 2. Aufl. 2018, Schmitz, S. 455, Rn. 22 zu § 13 TMG.

1050 *Bäcker,* Datenschutz-Grundverordnung, Raab, S. 1144, Rn. 11 zu Art. 95 DS-GVO.

transparent wie möglich formuliert werden. Dies entspricht der in Art. 6 Abs. 1 lit. a bezeichneten Anforderung, wonach die Einwilligung für einen oder mehrere bestimmte Zwecke erteilt werden muss, die der betroffenen Person gegenüber offenzulegen sind.[1051]

Erwägungsgrund 42

Erfolgt die Verarbeitung mit Einwilligung der betroffenen Person, sollte der Verantwortliche nachweisen können, dass die betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat. Insbesondere bei Abgabe einer schriftlichen Erklärung in anderer Sache sollten Garantien sicherstellen, dass die betroffene Person weiß, dass und in welchem Umfang sie ihre Einwilligung erteilt. Gemäß der Richtlinie 93/13/EWG des Rates sollte eine vom Verantwortlichen vorformulierte **Einwilligungserklärung** in **verständlicher** und **leicht zugänglicher Form** in einer **klaren und einfachen Sprache** zur Verfügung gestellt werden, und sie sollte **keine missbräuchlichen Klauseln beinhalten**. Damit sie in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen. Es sollte nur dann davon ausgegangen werden, dass sie ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.[1052]

Die DS-GVO macht deutlich, dass eine Einwilligung eine Erklärung oder eine eindeutige bestätigende Handlung von Seiten der betroffenen Person erfordert, was bedeutet, dass die Einwilligung stets durch eine aktive Handlung oder Erklärung erteilt werden muss. Die DS-GVO schreibt vor, dass eine „Erklärung oder eindeutige bestätigende Handlung" die Voraussetzung für eine „**ordnungsgemäße**" Einwilligung ist. Da die Anforderung einer „ordnungsgemäßen" Einwilligung in der DS-GVO bereits einen höheren Standard einnimmt, als das Erfordernis der Einwilligung in der Richtlinie 95/46/EG, muss geklärt werden, welche zusätzlichen Anstrengungen ein Verantwortlicher unternehmen sollte,

1051 *ARTIKEL-29-DATENSCHUTZGRUPPE,* Artikel-29-Datenschutzgruppe Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Guidelines/WP259_LeitlinienFuerDieEinwilligung.html.

1052 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Erwägungsgrund 42.

um eine ausdrückliche Einwilligung der betroffenen Person im Sinne der DS-GVO zu erhalten. ein, dass die betroffene Person in diese bestimmte Verarbeitung eingewilligt hat.[1053]

Der EuGH hat in seinem Urteil C-673/17 festgelegt, dass das Setzen von Cookies eine eindeutige Einwilligung des Internetnutzers erfordert. Ein voreingestelltes Ankreuzkästchen genüge in diesen Fällen nicht. Der EuGH stellt hier klar, dass die Einwilligung für jeden konkreten Fall erteilt werden muss. Weiterhin wurde ausgeführt, dass der Diensteanbieter gegenüber dem Nutzer in Bezug auf die Cookies, Angaben zur Funktionsdauer und zur Zugriffsmöglichkeit Dritter machen muss.[1054]

Die Auswahl von Cookies hat sich durch die aktuelle Datenschutz-Grundverordnung, verbunden mit der noch ausstehenden aktuellen ePrivacy-Richtlinie verändert. Zwischenzeitlich ist eine aktive Handlung erforderlich bei der Auswahl und Genehmigung von Cookies. Nachfolgende Grafik zeigt eine Variante der Auswahl benötigter und nicht benötigter Cookies.

1053 *ARTIKEL-29-DATENSCHUTZGRUPPE,* Artikel-29-Datenschutzgruppe Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Guidelines/WP259_LeitlinienFuerDieEinwilligung.html.

1054 EuGH, 01.10.2019 – C-673/17 http://curia.europa.eu/juris/.

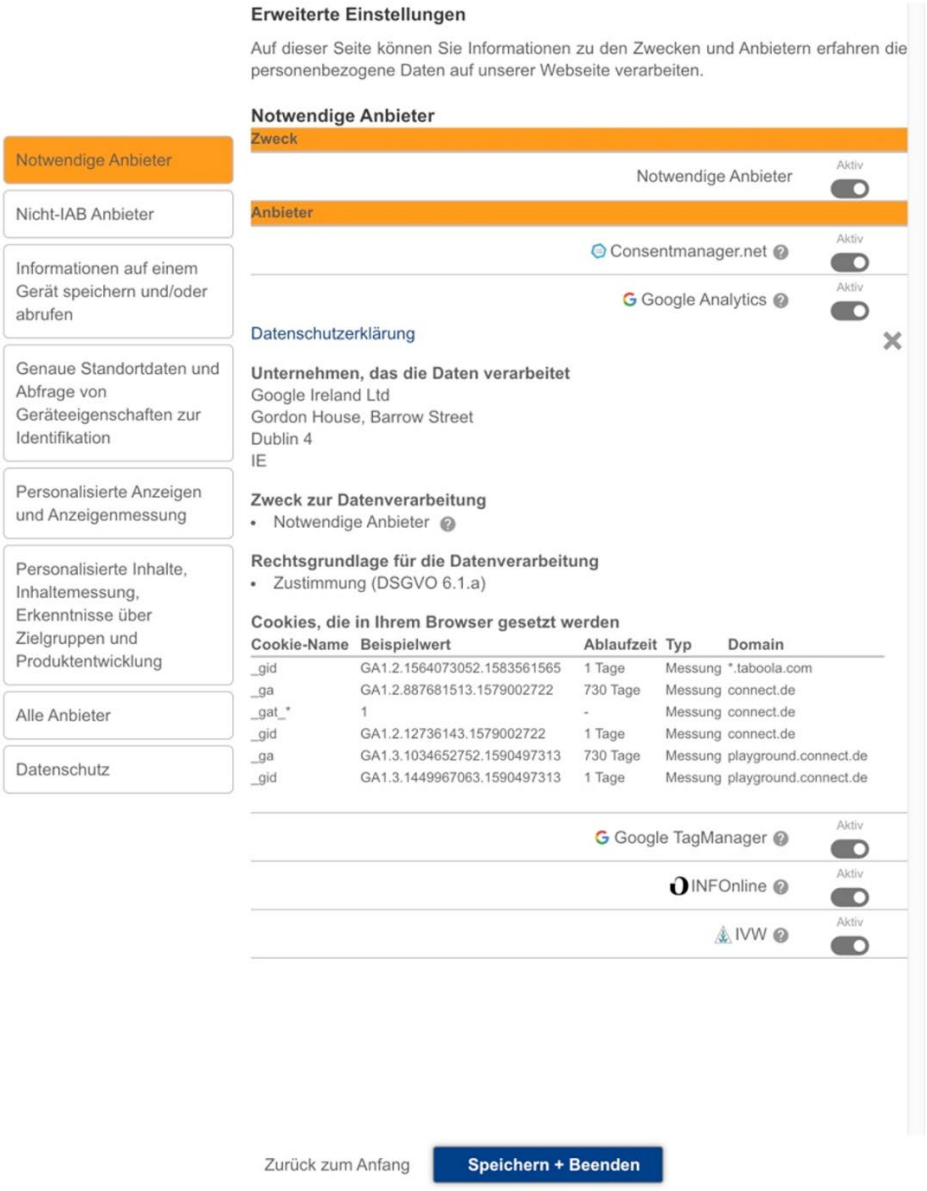

Abbildung 23: Cookie-Banner „Connect.de"-Banner

Wie dieser Abbildung zu entnehmen ist, handelt es sich um eine Übersicht über die eingesetzten Cookies der Onlinesite, „Connect.de" Dargestellt sind alle eingesetzten Cookies, die Kategorie, das Unternehmen sowie die Dauer des Einsatzes wie auch der Bezug zur Datenschutz-Grundverordnung. Auf diese erweiterte Ansicht gelangt der Nutzer allerdings erst, wenn er den Auswahlbutton hierfür betätigt. Mit der Akzeptierung der Cookies durch Anklicken des Einverständnis-Buttons, wird diese erweiterte Darstellung nicht erkennbar werden. Hierzu muss der wenig auffällige Einstellungen-Button gefunden und angeklickt werden. Da die meisten Nutzer weder die Zeit noch das

Interesse besitzen, die eingesetzten Cookies zu analysieren, wird in der Regel der Button zum Einverständnis betätigt werden.

Einige Webseitenanbieter benutzen aktuell Varianten, die ohne Cookies auskommen sollen oder können. Hierzu werden allerdings in einigen Fällen Abonnements oder Registrierungen abgeschlossen, die in der Folge den Verlust möglicher Werbeeinnahmen kompensieren sollen. Selbst in Fällen der nicht werbefinanzierten Webseitennutzung, in welchen personenbezogene Daten in Form von Namen, Adressen sowie Bezahldaten übertragen werden müssen, wird der datenschutzrechtliche Aspekt erneut nicht vollends berücksichtigt. Es existieren darüber hinaus Webseiten, die ohne den Einsatz von Cookies problemlos funktionieren (vgl. www.datenschutz-berlin.de).

Für den Fall, dass Cookies verwendet werden sollen oder müssen, befindet sich eine Muster-Vorlage für die Datenschutzerklärung für Webseiten im Anhang, unter Punkt IX dieser Arbeit.

2.9.5 TOM (Technisch Organisatorische Maßnahmen)

Der Gesetzgeber hat mit § 64 BDSG die ausführlichen Anforderungen an die Datensicherheit des Art. 29 JIRL[1055] bei Verarbeitung personenbezogener Daten durch Strafverfolgungs- und Gefahrenabwehrbehörden umgesetzt.[1056]

Mit Art. 29 JIRL hat der europäische Richtliniengeber einen etwas anderen Weg als der europäische Verordnungsgeber mit Art. 32 DS-GVO gewählt, die Sicherheit der Datenverarbeitung zu beschreiben. Der Gesetzgeber des BDSG, wie auch der Richtliniengeber der JIRL und der Verordnungsgeber der DS-GVO, versuchen mit der Beschreibung einer Vielzahl von Einflussfaktoren die gebotenen »technische und organisatorischen Maßnahmen« zu beschreiben. Dabei sind unter den **t**echnischen und **o**rganisatorischen **M**aßnahmen (**TOM**), die Sicherheitsvorkehrungen zu verstehen, mit denen sich eine Stelle durch Einrichtungen in der Hard- und Software (technische

1055 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) und zur Umsetzung der Richtlinie (EU) 2016/680, in: Bundesgesetzblatt,

1056 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, S. 1839, Rn. 1, § 64 BDSG.

Maßnahmen) oder durch Vorgaben gegenüber den Mitarbeitern vor unerwünschten Datenschutzvorfällen schützt.[1057]

Die acht Einflussfaktoren des § 64 Abs. 1 Satz 1 BDSG, wie auch gleichlautend des Art. 29 Abs. 1 JIRL (und des Art. 32 Abs. 1 DS-GVO) sind:

1. Der Stand der Technik,
2. Die Implementierungskosten,
3. Die Art der Verarbeitung,
4. Der Umfang der Verarbeitung,
5. Die Umstände der Verarbeitung,
6. Die Zwecke der Verarbeitung,
7. Die unterschiedlichen Eintrittswahrscheinlichkeiten von Nachteilen für die Betroffenen,
8. Die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.[1058]

Der Verantwortliche für die Verarbeitung personenbezogener Daten hat alle notwendigen technischen und organisatorischen Maßnahmen zu treffen, die nach der EU-DS-GVO und dem BDSG erforderlich sind.

Diese Grundsätze werden aus Sicht der Datenschutzbehörde nicht selten vernachlässigt und bilden immer wieder Anlass für öffentliche Kritik, Datenpannen und Skandale.[1059]

§ 64 Abs. 3 BDSG listet von Nr. 1 – 14, in Verwandtschaft zur Beschreibung der Datensicherheitsmaßnahmen in Anlage zu § 9 BDSG a.F. und ihren acht konkreten Sicherheitszielen, bestimmte Maßnahmen der Datensicherheit auf.

Dabei schafft der Gesetzgeber des BDSG – im Unterschied zu den zehn Maßnahmen des Richtliniengebers- **14 Sicherheitsmaßnahmen**, ergänzt durch die Maßnahme der Verschlüsselung.[1060]

1057 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Kramer/Meints, S. 490 Rn. 46f. Art. 32 DSGVO.
1058 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Kramer/Meints, S. 1839, Rn. 2.
1059 *Reimann/e.V.,* Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung, 2. Aufl. 2018, Kontrollbereich der technisch-organisatorischen Regelungen im Datenschutz, S. 68.
1060 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, S. 1840, Rn. 6.

Die 14 Kontrollbereiche können mithilfe einer Checkliste im Unternehmen kritisch hinterfragt werden.[1061]

Die **Sicherheitsmaßnahmen** im Datenschutz umfassen:

2.9.5.1 Zugangskontrolle (Abs. 3 Satz 1 Nr. 1 BDSG)

Unter Zugangskontrolle werden vor allem bauliche, technische oder organisatorische Maßnahmen verstanden, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren. Neben technischen Lösungen können an dieser Stelle organisatorische Regelungen helfen. Beispielsweise ist eine Zugangsmöglichkeit nur zu bestimmten Zeiten, in Anwesenheit einer zweiten Person oder mit Kameraüberwachung vorstellbar, auch wenn bei letzter Möglichkeit nur eine Rückverfolgbarkeit gewährleistet werden kann (Zugangsprotokollierung).[1062]

Die Zutrittskontrolle zielt darauf ab, den Zugang zu Datenverarbeitungssystemen physisch zu verhindern (z.B. durch bauliche Maßnahmen wie einbruchshemmende und durch Schlösser oder andere Zutrittskontrollsysteme gesicherte Türen).[1063] Ausgangspunkt ist zunächst die notwendige Festlegung, welche Personen berechtigterweise Zutritt zu welchen konkreten Datenverarbeitungsanlagen benötigen und für welche Zwecke sie dies dürfen.[1064] Die Einhaltung dieser Berechtigungen ist dann sicherzustellen. Baulich kann der Zutritt durch abgeschottete Räume mit verschließbaren Türen und Fenstern reguliert werden. Es kann auch angebracht sein, den Zutritt zu einzelnen Datenverarbeitungsanlagen innerhalb eines baulichen Raumes dadurch feingliedriger zu steuern, dass die Verarbeitungsanlagen ihrerseits durch technische Maßnahmen nochmals vor unbefugtem Zutritt geschützt werden (Sicherheitszonen). Dies ist z.B. in der Form denkbar, dass Serverschränke in nochmals durch Gitter abgetrennten Bereichen stehen oder die Serverschränke abschließbar sind. Solche Maßnahmen bieten sich z.B. an, wenn Dienstleister in einem Raum Datenverarbeitungsanlagen für

1061 *Reimann/e.V.,* Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung, 2. Aufl. 2018, S. 68, 5.2, 14 Kontrollbereiche der technisch-organisatorischen Regelungen im Datenschutz, vgl. Formular Technisch Organisatorische Maßnahmen im Anhang.

1062 *Reimann/e.V.,* Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung, 2. Aufl. 2018, S. 70 Abschnitt 5.2.1 Zugangskontrolle.

1063 *Simitis/Dammann/Arendt* (Hrsg.), Bundesdatenschutzgesetz, § 9 BDSG, Rn. 77.

1064 *Simitis/Dammann/Arendt* (Hrsg.), Bundesdatenschutzgesetz, § 9 BDSG, Rn. 79.

verschiedene Kunden betreiben. Jeder Zutritt zu den Anlagen sollte protokolliert werden.[1065]

2.9.5.2 Datenträgerkontrolle (Abs. 3 Satz 1 Nr. 2 BDSG)

Zugangskontrolle soll das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern verhindern.[1066]

Hierzu werden unterschiedliche Maßnahmen eingesetzt:

- Geeignete Arten der Authentifizierung wie bspw. eine sog. ein - oder Mehr-Faktor Authentifizierung,
- Vorgaben für den sicheren Gebrauch von Passwörtern,
- Berechtigungsmanagement,
- Sperrung von Konsolen,
- Nach Beendigung der Tätigkeit an Terminals oder Systemen sollten Benutzer sich abmelden,
- Zeitnahes Schließen von Sicherheitslücken in Betriebssystemen und Anwendungen,
- Schutz vor Schadsoftware.[1067]

2.9.5.3 Speicherkontrolle, Eingabekontrolle (Abs. 3 Satz 1 Nr. 3 und 7 BDSG)

Nachträglich kann überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Im Zusammenhang mit der Eingabekontrolle hat sich die Wortschöpfung eines Wirtschaftsprüfers seit einigen Jahren durchgesetzt, Revisionssicherheit. Folgende grundsätzlichen Kriterien gelten nach Kampffmeyer für die Revisionssicherheit von Archivierungssystemen:[1068] Ordnungsmäßigkeit, Vollständigkeit, Sicherheit des Gesamtverfahrens, Schutz vor Veränderung und Verfälschung, Sicherung vor Verlust, Nutzung nur durch Berechtigte, Einhaltung der Aufbewahrungsfristen, Dokumentation

---

1065 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Rn. 39, Position 38928 von 87533.

1066 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Kramer/Meints, S. 1844, Rn. 16 (Datenträgerkontrolle nach § 64 Abs. 3 Satz 1 Nr. 2 BDSG).

1067 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Kramer/Meints, S. 1844 und 1845, Rn. 16 (Datenträgerkontrolle nach § 64 Abs. 3 Satz 1 Nr. 2 BDSG).

1068 *Kampffmeyer, Ulrich*, http://www.project-consult.de/files/S 113EIA_H_2013. pdf, S. 17 ff., Revisionssicherheit von Archivierungssystemen, Eingabekontrolle, Plausibilitätskontrolle, Transaktionskontrolle 2013.

des Verfahrens, Nachvollziehbarkeit, Prüfbarkeit. Die Eingabekontrolle selbst setzt eine wirksame Zugangs- und Zugriffskontrolle voraus. Eine funktionierende Eingabekontrolle besteht nicht nur aus organisatorischen Maßnahmen, sondern erfordert auch ein technisches Verfahren. Dieses technische Verfahren kann entweder in der Applikation selbst vorhanden sein oder durch ein entsprechendes Zusatzsystem, welches der Applikation hinzugefügt wird, realisiert werden. Die beste technische Lösung funktioniert natürlich nur, wenn sie verbunden ist mit zuverlässiger Organisation der Kontrolle und Auswertung der Eingabekontrolle, z. B. dem Vier-Augen-Prinzip.[1069]

Die Speicherkontrolle soll die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Verändern und Löschung von gespeicherten Daten verhindern. Die Eingabekontrolle soll gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogene Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden.[1070]

2.9.5.4 Benutzerkontrolle–Zugriffskontrolle (Abs. 3 Satz 1 Nr. 4 und 5 BDSG)

Es wird gewährleistet, dass die Berechtigten ausschließlich auf die Daten zugreifen können, für die sie eine Zugriffsberechtigung besitzen (need-to-know-Prinzip) und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der Zugriff auf personenbezogene Daten wird kontrolliert, indem dieser in Logdateien des Systems manipulationssicher protokolliert wird. Wenn sich eine befugte Person in einem Raum mit einer Datenverarbeitungsanlage befindet und das System benutzt, muss sichergestellt sein, dass sie nur auf die Daten zugreifen kann, für die sie die entsprechende Berechtigung besitzt (Berechtigungskonzept). Dabei muss nachvollziehbar sein, wer wann auf welche Daten zugegriffen hat.[1071]

2.9.5.5 Übertragungskontrolle / Transportkontrolle (Abs. 3 Satz 1 Nr. 6 BDSG)

Personenbezogene Daten dürfen bei der elektronischen Übertragung oder während des Transportes nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden. Es

---

1069 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, Müller, S. 485, Nr. 32.

1070 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Kramer/Meints, S. 1846, Rn. 17 (Speicherkontrolle und Eingabekontrolle, § 64 Abs. 3 Satz 1 Nr. 3 und 7 BDSG).

1071 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, S. 482, Rn. 21, (Zugriffskontrolle Art. 32, 25 DSGVO sowie Kramer/Meints in Auernhammer, S. 1844 Rn. 16 § 64 Abs. 3 Satz 1 Nr. 2 BDSG).

muss jederzeit überprüfbar und feststellbar sein, an welchen Stellen eine Übermittlung personenbezogener Daten vorgesehen ist. Technisch ist dies durch eine Verschlüsselung bei der Übertragung zu erreichen, was in Art. 32 Abs. 1 lit. a DS-GVO explizit gefordert wird. Die Sicherheit von Daten ist in der Praxis besonders kritisch bei E-Mail-Verkehr, Nutzung von Funknetzen, Transport von Datenträgern oder bei Ausdrucken auf Papier. Maßnahmen im Bereich der Weitergabekontrolle sind daher insbesondere in diesen Bereichen zu kontrollieren (ist der Einsatz von SSL / HTTPS-verschlüsselter Übertragung möglich oder ein VPN-vorhanden?). Die Überprüfbarkeit und Feststellbarkeit, an welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Übertragung von Daten vorgesehen ist, stellt sich in der Praxis insbesondere bei der Nutzung von Fernwartungszugängen auch für Telekommunikationsanlagen (neuerlich auch über All-IP), Backup-Datenleitungen, Funk-Netzwerke, Infrarot- und Bluetooth-Netze sowie im Mobilfunk als besonders problematisch dar.[1072]

2.9.5.6 Wiederherstellbarkeit (Abs. 3 Satz 1 Nr. 9 BDSG)

Eine vertragliche Regelung über Art, Umfang und Aufbewahrungsdauer muss vorhanden sein. Ist zum Zeitpunkt der Prüfung kein Datensicherungsverfahren festgelegt, ist umgehend ein solches zu erstellen und von beiden Seiten als Vertragsanlage zu unterzeichnen.[1073]

Hierzu können folgende Methoden verwendet werden:

- Redundante Systeme mit mehreren Festplatten (Blades)
- Geeignete Software mit standardisierten und regelmäßigen Backups,
- Einsatz von Cloud Systemen, um ein hardwareunabhängiges Medium verwenden zu können.
- Datensicherungsverfahren auf Basis „Großvater-Vater-Sohn“

Das Datensicherungsprinzip „**Großvater-Vater-Sohn**“ ist ein zuverlässiges und weltweit eingesetztes Rotationsverfahren zur Sicherung von Daten auf Speichermedien. Die erste Generation bildet die tägliche Sicherung („Sohn“). Für jeden Wochentag erfolgt

---

1072 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, Müller, S. 484, Nr. 24 (§ 64 Abs. 3 Satz 1 Nr. 6 und 8 BDSG, Art. 32, 25 DSGVO).

1073 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, Müller, S. 488, Nr. 46 (Art. 32, 25 DSGVO, siehe auch § 64 Abs. 3 Satz 1 Nr. 9 BDSG).

eine inkrementelle oder differenzielle Sicherung auf ein eigenes Speichermedium. Das heißt, es werden nur diejenigen Daten gesichert, die geändert wurden oder hinzugekommen sind. Einmal wöchentlich erfolgt eine Vollsicherung, meist Freitag, ebenfalls auf jeweils einem eigenen Medium. Die Vollsicherung stellt die zweite Generation dar („Vater"). Zum Monatsanfang wird die Wochensicherung aus dem Rotationsverfahren entnommen und dem Monatszyklus hinzugefügt, die dritte Generation („Großvater"). Zum Ende des Jahres wird aus dem Monatszyklus die Jahressicherung (vierte Generation) entnommen und sicher aufbewahrt.[1074]

2.9.5.7 Zuverlässigkeit (Abs. 3 Satz 1 Nr. 10 BDSG)

Die Zuverlässig soll gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.[1075] Hierzu dienen so genannte Monitoring Systeme, die auftretende Probleme zeitnah melden, um dadurch einen möglichen Ausfall korrigieren oder gar verhindern zu können.

2.9.5.8 Datenintegrität (Abs. 3 Satz 1 Nr. 3 BDSG)

Mit dem Begriff der Integrität ist gemeint, dass die Unversehrtheit der Daten sichergestellt und unbefugte Veränderungen der Daten verhindert werden.[1076] Risiken für die Integrität der Systeme und Dienste drohen vor allem durch externe Angreifer. Diese nutzen oft Schadsoftware, um Daten auf fremden Systemen zu verändern – die Systeme und Dienste also manipulieren zu können. Oftmals sind Systeme und Dienste gegen unbefugte Zugriffe aber nicht ausreichend geschützt (z.B., weil unsichere Passwörter verwendet werden) und Angreifer können ohne Nutzung einer Schadsoftware Zugriff erlangen.[1077]

2.9.5.9 Auftragskontrolle (Abs. 3 Satz 1 Nr. 12 BDSG)

Bei der Auftragskontrolle wird gewährleistet, dass die personenbezogenen Daten, die im Auftrag verarbeitet werden, nur auf Grundlage des Vertrages entsprechend den

---

1074 *Little/Chapa,* Implementing backup and recovery, 2003, Chapter 2, Business Requirements of Backup Systems, Page. 17 f. (aus dem Englischen Koreng / Müller, S. 488 Nr. 47).

1075 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Kramer/Meints, S. 1850, Rn. 22 (§ 64 Abs. 3 Satz 1 Nr. 10 BDSG).

1076 *Kutscha, Martin*, Das „Computer-Grundrecht" — eine Erfolgsgeschichte?, zum Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 - - 1 BvR 595/07 -, in Datenschutz Datensich 2012, 391.

1077 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Rn. 45, Position 39017 von 87533.

Weisungen des Auftraggebers (Verantwortlichen) verarbeitet werden. In Art. 28 Abs. 3 lit. a DS-GVO wird klargestellt, dass die Auftragsverarbeitung durch den Auftragsverarbeiter (Auftragnehmer) nur auf „dokumentierte Weisung des Verantwortlichen“ durchgeführt werden darf.[1078]

Hierzu sollten folgende Maßnahmen umgesetzt werden:

- Vertragliche Gestaltung,
- Angemessene und geeignete organisationsübergreifende Prozesse zur Steuerung und Dokumentation von Aufträgen,
- Regelmäßige Kontrollen der Systeme durch entsprechende Audits.

2.9.5.10 Verfügbarkeitskontrolle (Abs. 3 Satz 1 Nr. 13 BDSG)

Personenbezogene Daten sind gegen Zerstörung oder Verlust zu schützen. Die Verfügbarkeit der Daten wird kontrolliert, d. h. es wird sichergestellt, dass die personenbezogenen Daten zu festgelegten Zeiten im festgelegten Umfang zur Verfügung gestellt werden. Die Verfügbarkeit selbst muss dabei den rechtlichen und betrieblichen Erfordernissen entsprechen, so dass u. a. bei Wartungsfenstern für die Pflege und Wartung der Systeme und Software, diese den laufenden Betrieb nicht negativ beeinflussen.[1079]

2.9.5.11 Trennungskontrolle, Mandantentrennungskontrolle (Abs. 3 Satz 1 Nr. 14 BDSG)

Die Vorgabe zu Datentrennung soll sicherstellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.[1080] Dies ist beispielsweise von großer Bedeutung im Bereich der Marktforschung oder für andere Forschungszwecke, wenn mehrfach Daten bei einer Person für unterschiedliche Zwecke erhoben werden. Ein weiterer wichtiger Anwendungsbereich ist in Unternehmen, die Kundenbeziehungs-software (CRM-Systeme) einsetzen. Eine Vermischung oder anders geartete

---

1078 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, Müller, S. 486, Nr. 38 (Art. 32, 25 DSGVO, siehe auch § 64 Abs. 3 Satz 1 Nr. 12, Rn. 24 BDSG in Auernhammer, Kramer/Meints.

1079 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, S. 486, Nr. 39.

1080 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Kramer/Meints, S. 1853, Rn. 26 (§ 64 Abs. 3 Satz 1 Nr. 14 BDSG, Trennbarkeit).

Verarbeitung sowie insbesondere eine Datenanreicherung zu den personenbezogenen Daten muss durch technische Maßnahmen vermieden werden.[1081]

2.9.5.12 Verschlüsselungsverfahren

Art. 6 Abs. 3 lit. e und Art. 32 Abs. 1 lit. a DS-GVO fordern eine Verschlüsselung der personenbezogenen Daten zum Schutz dieser Daten. Hierzu fordert das BSI ein erhöhtes Sicherheitsniveau von 120 Bit ab dem Jahr 2023 in der Änderung seiner derzeitigen Krypto-Richtlinien der Serie TR–02102.[1082]

2.9.5.13 Verwendung von Passwörtern

Die Handhabung der Passwortvergabe, -nutzung und -änderung, insbesondere bei nicht sensiblen Daten, weicht in der Praxis häufig von den gesetzlichen Vorgaben zum Zugang und Zugriff auf personenbezogene Daten ab. Nicht selten wird auf die Vergabe von personenbezogenen Passwörtern zugunsten von Gruppenkennungen verzichtet. Eine Rückverfolgbarkeit von unerlaubten Datenzugriffen ist damit natürlich nicht mehr möglich. Eine wesentliche Aufgabe des Datenschutzbeauftragten besteht deshalb darin, die Passwortvergabe im Unternehmen zu verifizieren. Ein sicherer Zugangs- und Zugriffsschutz kann nur dann gewährleistet werden, wenn:[1083]

- jeder Benutzer über ein eigenes Passwort verfügt,
- ein technisches System die Änderung des Passworts spätestens nach 90 Tagen fordert,
- der Benutzer das Passwort jederzeit wieder ändern kann,
- die letzte Änderung des Passworts für den Benutzer angezeigt wird und
- die Änderungshistorie systemtechnisch nachvollziehbar ist.

Das Passwort selbst muss zur Gewährung eines wirksamen Zugangs- und Zugriffsschutzes bestimmte Anforderungen erfüllen. In der Praxis hat sich gezeigt, dass

---

1081 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, Müller, S. 488, Nr. 53 (Art. 32, 25 DSGVO, siehe auch Auernhammer S. 1853, Rn. 26).

1082 Bundesamt für Sicherheit in der Informationstechnik, Krypto-Richtlinien, BSI aktualisiert Krypto-Richtlinien der Serie TR-02102, erhöhtes Sicherheitsniveau von 120 Bit ab 2023 20.03.2017, https://www.bsi.bund.de/DE/Presse/Pressemitteilugen/Presse2017/Aktualisierte_Krypto-Richtlinien_TR–02102_20032017.html).

1083 *Reimann/e.V.,* Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung, 2. Aufl. 2018, S. 73, Verwendung von Passwörtern.

viele Benutzer entweder die Namen, Geburtsdaten ihrer nächsten Verwandten oder Wörter aus ihrer unmittelbaren Arbeitsumgebung nutzen. Folglich sind diese schnell zu erraten. Gute Passwörter weisen hin-gegen eine Mindestlänge von 8 Zeichen auf und enthalten Ziffern oder Sonderzeichen. Regeln für ein gutes Passwort sollten Mitarbeitern in Schulungen oder in Anweisungen bekannt gemacht werden.

2.9.5.14 Biometrische Zugangskontrolle

Der Begriff „Biometrie“ ist eine aus dem Griechischen hergeleitete Wortkombination aus ***bios (= Leben) und metron (= Maß).*** Das Fachgebiet der Biometrie befasst sich mit Messungen an Lebewesen und den damit verbundenen Mess- und Auswerteverfahren. Es untergliedert sich in die Teilgebiete der biometrischen Statistik und der biometrischen Erkennungsverfahren.[1084]

Der Login der Zukunft kommt ohne Passwörter aus. Zu aufwendig ist die Handhabung von Passwörtern, zu groß das Risiko, das durch triviale oder mehrfach genutzte Passwörter entsteht. Ein Weg könnte die Authentifikation per Mobil-Telefon (Handy) sein, eine andere Alternative zum Passwort ist der Zugriffsschutz mit Hilfe biometrischer Merkmale, wie etwas Fingerabdruck oder per Gesichtserkennung.[1085] Im Mittelpunkt steht dabei die automatische Erkennung von Individuen.[1086]

1084 *A. Albrecht,* Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, 2003, Allgemeine Informationen.

1085 *Rimscha, Markus von*, Datenschutz - Konzepte, Algorithmen und Anwendung, Werkzeuge zum Datenschutz im Alltag, 2018.

1086 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kramer, S. 450, Rn. 1.

In der praktischen Anwendung biometrischer Verfahren zur automatisierten Erkennung von Personen können folgende biometrische Charakteristika Gegenstand der Überprüfung sein:[1087]

- Körpergröße,
- Gesichtsgeometrie,
- Körpergeruch,
- Gangstil,
- Stimme,
- Lippenbewegung,
- Hand- und Unterschrift,
- Tippverhalten aus Tastaturen,
- Regenbogenhaut / Iris des Auges,
- Retina (Augenhintergrund),
- Fingerabdruck,
- Ohrform,
- Handgeometrie,
- Handgefäßstruktur,
- Handlinienstruktur,
- Zahnabdruck,
- Nagelbettmuster.

Wie sich aus den beispielhaft aufgezählten Merkmalen ergibt, handelt es sich um physiologische und verhaltensbezogene Daten.[1088] Nach Art. 4 Nr. 14 DS-GVO und § 46 Nr. 12 BDSG sind biometrische Daten „*mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie insbesondere Gesichtsbilder oder*

1087 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kramer, S. 450, Rn. 2.

1088 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kramer, S. 451, Rn. 3 Satz 1.

daktyloskopische Daten".[1089] Die Verarbeitung biometrischer Daten ist nach Art. 9 Abs. 1 DS-GVO **grundsätzlich untersagt**.

Die neue Schutzkategorie der eindeutig identifizierenden Biometriedaten (Art. 4. Nr. 14 DS-GVO) hat einen spezifisch datenschutzrechtlichen Hintergrund. Damit soll das Erstellen umfassender Persönlichkeitsprofile durch systematische Zusammenführung von Daten mit Hilfe dieser mit modernen technischen Mitteln einfach zu erlangenden und vom Betroffenen nicht beeinflussbaren Daten verhindert werden.[1090]

Da die **Arbeitswelt 4.0** sensible Bereiche kennt, deren Zugang und Zutritt explizit überprüft und überwacht werden müssen, existieren auch für die biometrischen Verfahren, Ausnahmen, welche in Art. 9 Abs. 2 DS-GVO sowie § 22 und in § 26 Abs. 3 BDSG, geregelt sind. Dieses wiederum unterliegt der Freiwilligkeit und deren sonstigen Wirksamkeitsvoraussetzungen. Die Einwilligung muss ausdrücklich und konkret die Zwecke und die betroffenen biometrischen Merkmale benennen.[1091]

2.9.5.15 Identifizierbarkeit der Internet Nutzer

Die technische Infrastruktur des Internets leistet einen Beitrag zur möglichen Identifizierung von Benutzern. Grundlage hierfür sind die den angeschlossenen Rechnern zugeordneten IP-Adressen[1092]. Da diese durch den Access Provider dem entsprechenden Rechner zugewiesen wird, kann aufgrund der geschlossenen Verträge auf die persönlichen Daten zugegriffen werden. Mit einer entsprechenden Zuordnung kann das Nutzungsprofil des entsprechenden Vertragspartners zur Überprüfung herangezogen werden, dass dieser Vertragspartner zu einem bestimmten Zeitpunkt unter einer bestimmten IP-Adresse online war. So bildet die IP-Adresse den Ausgangspunkt für eine auf die Identifizierung eines Internet-Benutzers gerichtete Beweisführung, diese

1089 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kramer, S. 453, Rn. 9, Satz 1.
1090 *Bäcker,* Datenschutz-Grundverordnung, S. 300, Rn. 32 (Art. 9 DSGVO).
1091 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kramer, S. 453, Praxishinweis, Rn. 9.
1092 *CZERNIK, AGNIESZKA*, IP-Adressen – Funktion, Aufbau, Tracking, IP-Adresse - Internet Protokoll Adresse, https://www.datenschutzbeauftragter-info.de/ip-adressen-funktion-aufbau-tracking/.

allerdings – soll sie rechtlich Bestand haben – noch verschiedene juristische Bewertungen voraussetzt.[1093]

Die technischen Gegebenheiten einer „IP-Adresse“ sind somit, ohne Hinzutreten weiterer Umstände, keine hinreichende Bedingung für die Identifizierung eines Internet-Nutzers. Aus dem Status der IP-Adresse erklärt sich auch die Debatte darüber, ob sie als personenbezogenes Datum angesehen werden kann.[1094]

Bezogen auf Daten und Persönlichkeitsschutz zählt nicht nur die Tatsache, dass im Internet einschlägige Informationen vorhanden sind, sondern vor allem die Tatsache, dass diese mit Hilfe der verfügbaren Suchmaschinen, zielgerichtet gesucht und gefunden werden können. Bezüglich der im Internet vorhanden Informationen wird verschiedentlich darauf hingewiesen, dass diese dauerhaft verfügbar seien und dass dies **datenschutzrechtliche Konsequenzen** nach sich ziehen müsse.[1095]

Viele Webseiten nutzen **Tracking-Tools**, um Nutzerbewegungen auf ihrer Seite auszuwerten. Hierzu wird die IP-Adresse verwendet. Seit längerem besteht Streit darüber, ob IP-Adressen für den Website-Betreiber einen Personenbezug haben. Bei statischen IP-Adressen wird dies überwiegend bejaht, bei dynamischen IP-Adressen wird heftig über den Personenbezug gestritten. Wichtig ist diese Frage deswegen, weil ein Personenbezug der IP-Adresse zur Folge hat, dass diese über den bloßen Verbindungsaufbau hinaus ohne Einwilligung eines jeden Surfers nicht verwendet werden darf.

Deswegen muss derzeit beim Einsatz der Tracking-Tools die IP-Adresse anonymisiert werden. Die meisten Tools löschen deswegen die letzten 8 Bits der IP-Adresse. Da der Netzwerkanteil bei der Anonymisierung erhalten bleibt, ist es aber weiterhin möglich auszuwerten, aus welchem Gebiet ein Rechner auf die Webseite zugreift.[1096]

Die Frage, inwieweit IP-Adressen einen Personenbezug aufweisen, hat der **BGH** (**B**undes**g**erichts**h**of) dem **Eu**ropäischen **G**erichts**h**of (**EuGH**) vorgelegt. Es bleibt

---

1093 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Herberger, S. 111, Rn. 4a.

1094 Zweite Kammer, 19 Oktober 2016 – In der Rechtssache C-582/14 (2016).

1095 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Herberger, S. 113, Rn. 14, Satz 1.

1096 *CZERNIK, AGNIESZKA*, IP-Adressen – Funktion, Aufbau, Tracking, IP-Adresse - Internet Protokoll Adresse, https://www.datenschutzbeauftragter-info.de/ip-adressen-funktion-aufbau-tracking/.

abzuwarten, wie der Streit entschieden wird und ob dies noch eine Relevanz haben wird. Denn mit der Umstellung von IPv4 (Internet Protokoll Version 4) auf IPv6 (Internet Protokoll Version 6) werden 128-Bit Adressen verwendet. Das hat zur Folge, dass „jedes Sandkorn eine eigene IP-Adresse“ bekommen kann. Jedes Gerät (ob Rechner, internetfähige Kühlschränke, Autos, Fernseher) kann dauerhaft mit einer eigenen IP-Adresse versorgt werden, so dass keine dynamischen IP-Adressen verwendet werden müssen. Das heißt aber auch, dass das Tracking einzelner Geräte dadurch einfacher wird und das Surfen im Internet ohne Weiteres nicht mehr anonym erfolgen kann.[1097]

1097 *CZERNIK, AGNIESZKA*, IP-Adressen – Funktion, Aufbau, Tracking, IP-Adresse - Internet Protokoll Adresse, https://www.datenschutzbeauftragter-info.de/ip-adressen-funktion-aufbau-tracking/.

2.10 Arbeitnehmerdatenschutz

Der deutsche Gesetzgeber hat die Einwilligung im Beschäftigungsverhältnis zum 25.05.2018 in § 26 Abs. 2 BDSG ausdrücklich geregelt und somit die bisherige Auffassung in Rechtsprechung und Teilen der Literatur bestätigt. Die Norm stellt im Verhältnis zu den allgemeinen Vorschriften des Art. 7 DS-GVO über die Einwilligung eine spezifische Vorschrift im Beschäftigungskontext gem. Art. 88 Abs. 1 DS-GVO dar.[1098]

2.10.1 Arbeitnehmerdatenschutz im Rückblick

1884 kam Kodaks „Snap Kamera" auf den Markt. Jeder konnte in der Folge außerhalb von Fotostudios mit einer kleinen tragbaren Kamera Fotos „schießen". Die amerikanischen Anwälte Louis Brandeis und Samuel Warren suchten Abwehransprüche gegen Fotografen, die ohne Einwilligung Fotos von Dritten machten. Sie gaben ihrer 1890 angestellten Untersuchung den wegweisenden Titel „**The Right to Privacy**"[1099]. Demnach steht jedem Individuum das Recht zu, selbst zu bestimmen, inwieweit seine „Gedanken, Meinungen und Gefühle", anderen mitgeteilt werden sollen. Das war die Entdeckung des Rechts auf Schutz personenbezogener Informationen.[1100]

Rückblickend ist zu erwähnen, dass das von Beiden eingebrachte Gesetz vor dem amerikanischen Kongress scheiterte. Erst im Jahr 1974 kam es zur Verabschiedung des Privacy Act. Deutschland hingegen hatte bereits 1907 eine gesetzliche Grundlage verabschiedet. Das Gesetz betraf das Urheberrecht an Werken der bildenden Künste und der Fotografie (KunstUrhG) vom 9.1.1907. Der aktuell noch geltende **§ 22 KunstUrhG** führt aus:

Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, dass er sich abbilden ließ, eine Entlohnung erhielt. Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von 10 Jahren der Einwilligung der Angehörigen

---

1098 *Walter,* Datenschutz im Betrieb - DS-GVO in der Personalarbeit, 2018, S. 121, Abschnitt 7.1.

1099 *Warren, Samuel D., Brandeis, Louis D.*, Harvard Law Review Vol. IV. December 15, 1890. No. 5. The Right to Privacy, 23. Juli 2015.

1100 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, S. 1, Rn. 1, Die Entwicklung des Arbeitnehmerdatenschutzes.

des Abgebildeten. Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Abgebildeten und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Abgebildeten.[1101]

Auslöser war, dass zwei Fotographen sich Zutritt zum Sterbezimmer des Reichskanzlers, ***Otto von Bismarck*** verschafft hatten, Fotos gemacht hatten und diese veröffentlichen wollten. Aufgrund dieses Skandals entstand die erste deutsche Norm über die informationelle Selbstbestimmung.[1102]

2.10.2 Arbeitswelt 4.0

Mit dem Zukunftsprojekt „Industrie 4.0“, welches ein zentrales Element der Hightech- / Innovations-Strategie der Bundesregierung darstellt, soll die Informatisierung der klassischen Industrien, wie z. B. der Produktionstechnik, vorangetrieben werden. „Auf dem Weg zum Internet der Dinge soll durch die Verschmelzung der virtuellen mit der physikalischen Welt zu Cyber-Physical Systems und dem dadurch möglichen Zusammenwachsen der technischen Prozesse mit den Geschäftsprozessen der Produktionsstandort Deutschland in ein neues Zeitalter geführt werden.“[1103]

Verfolgte man den Prozess der Diskussion rund um das Zukunftsprojekt Industrie 4.0, zunächst im Kreis der Promotorengruppe Kommunikation innerhalb der Forschungsunion und dann in Vertiefung im gleichnamigen Arbeitskreis unter dem Vorsitz von Henning Kagermann (Deutsche Akademie der Technikwissenschaften acatech) und Siegfried Dais (Robert Bosch Industrietreuhand KG), so konnte man feststellen, dass sehr intensiv auch über die Wirkungen von Industrie 4.0 auf die Qualität der Arbeit, die Qualifikationserfordernisse, neue Formen der Arbeitsorganisation und Veränderungen im Zusammenspiel zwischen Mensch und Technik nachgedacht wurde. Zunächst unter der nicht ganz glücklich gewählten Überschrift „Faktor Mensch“,[1104] dann „Mensch und Arbeit“ befasste man sich mit dem absehbaren Paradigmenwechsel in der Mensch–Technik- und Mensch–Umgebungs-Interaktion und den damit verbundenen

---

1101 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie, § 22 KunstUrhG.

1102 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, S. 2, Rn. 2.

1103 *Botthof/Hartmann* (Hrsg.), Zukunft der Arbeit in Industrie 4.0, Position 126, Zukunft der Arbeit im Kontext von Autonomik und Industrie 4.0.

1104 *Promotorengruppe Kommunikation der Forschungsunion Wirtschaft - Wissenschaft*, Im Fokus: Das Zukunftsprojekt Industrie 4.0 - Handlungsempfehlungen zur Umsetzung, März 2012.

neuartigen Formen der kollaborativen Fabrikarbeit. In der Überzeugung, dass auch die Smart Factory im Rahmen von Industrie 4.0 keineswegs menschenleer sein wird, wurden zudem die Anforderungen an die Fähigkeiten und das Wissen von Beschäftigten in einem sich verändernden Arbeitsumfeld, bestimmt von komplexen Prozessen, technologisch anspruchsvollen Anlagen und Werkzeugen, ausführlich thematisiert. Neben kurz- und mittelfristigen Handlungsfeldern (bspw. Assistenzsysteme als „Fähigkeitsverstärker" physischer und kognitiver Leistungen, kollaborative industrielle Serviceroboter, Apps für eine software-basierte Konfiguration von Anlagen oder auch AR-Technologien zur schnellen Einweisung in Fertigungsprozesse oder zur Lernunterstützung) wurde eine Qualifizierungsinitiative vorgeschlagen, die sowohl die gewerbliche als auch hochschulische Aus- und Weiterbildung adressiert.[1105]

Die vorstehenden Ausführungen zur Arbeitswelt 4.0 zeigen, dass diese gekennzeichnet ist durch den Einsatz moderner Kommunikationsmittel und die Verarbeitung zahlreicher Daten der Arbeitnehmer. Wollte man mit der Terminologie des Datenschutzrechts sprechen, ist die Arbeitswelt 4.0 geprägt durch die Verarbeitung **großer Mengen personenbezogener Beschäftigungsdaten im Beschäftigungskontext**.[1106]

Daten und Persönlichkeitsschutz müssen die Sachverhalte möglicher Rechtsbeeinträchtigungen für Arbeitnehmer erfassen und rechtlich bewerten. Ein erster Punkt, der eine durch IT vermittelte Verletzung des Persönlichkeitsrechts beinhalten kann, ist das Tracking von Mitarbeitern. Tracking bedeutet in diesem Zusammenhang eine Nachführung des Verhaltens von Mitarbeitern. Und dies gefolgt von einer Verhaltensanalyse, welche Personalmaßnahmen für den einzelnen Arbeitnehmer oder eine Abteilung nach sich ziehen kann.[1107]

1105 *Botthof/Hartmann* (Hrsg.), Zukunft der Arbeit in Industrie 4.0, Position 126 Abs. 2.
1106 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, S. 33, Rn. 11, Teil A, Abschnitt 2.
1107 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Wächter, S. 132 Rn. 6.

2.10.3 Personalplanung

Personalplanung ist die gedankliche Vorstrukturierung von zielorientierten Entscheidungs- und Handlungsprogrammen in personellen Angelegenheiten, die auf der Basis von Antizipation zukünftiger und damit auch ungewisser Zustände und Entwicklungen entworfen werden. Es wird von betrieblicher oder unternehmerischer Personalplanung gesprochen, wenn die Planung von globalen oder detaillierten Personalproblemen in Betrieben bzw. Unternehmungen stattfindet.[1108]

Der Begriff Personalplanung lässt sich grob in folgende Teilbereiche gliedern:

- Personalbedarfsplanung
- Personalbeschaffungsplanung
- Personalgewinnungsplanung
- Personalentwicklung
- Personalfreisetzung

2.10.3.1 Personalbedarfsplanung

Die Personalbedarfsplanung oder auch Kapazitätsplanung ist von hoher, strategischer Relevanz und verfolgt das Ziel, auf Grundlage der Planungsparameter einen Abgleich zwischen Unternehmenszielen und Personalplänen zu schaffen.[1109]

Die lokale Dimension des Personalbedarfs bildet die räumliche oder regionale Reichweite des Erfassungsbereichs ab. In aufsteigender Reichweite wären etwa die organisatorischen Einheiten:

- Stelle
- Abteilung
- Hauptabteilung
- Bereich
- Sparte
- Einzelunternehmung
- Dezentralisierte nationale und multinationale Unternehmung,

---

1108 Wirtschafts-Lexikon, 2006, Mag, S. 4453, Abschnitt 1 - Begriff und Aufgabe der Personalplanung - Band: Med - Per (08).

1109 *Springer Gabler Verlag* (Hrsg.), Personalbedarfsermittlung, Gabler Wirtschaftslexikon, https://wirtschaftslexikon.gabler.de/definition/personalbedarfsermittlung-46363/version-269645.

zu nennen.

Die zeitliche Dimension legt fest, bis zu welchem Planungshorizont Bedarfsprognosen erstellt werden sollen. Bei der qualitativer Dimension geht es um die Ableitung von Anforderungen an Kenntnisse, Fertigkeiten und Verhaltensweisen aus zukünftigen teilaufgaben, die nur durch entsprechende Qualifizierungen des Personals erfüllt werden können. Hingegen bei der quantitativen Dimension geht es schlicht um die Anzahl der Personen.

2.10.3.2 Personalbeschaffungsplanung

Wird bei der Bedarfsplanung festgestellt, dass der aktuelle und künftige Bedarf an Personal angepasst werden muss, so geht es um die Frage, mit welchen Mitteln und auf welchem Wege die Anpassung erfolgen kann. Dabei werden grundsätzlich zwei Varianten unterschieden: interne und externe Personalbeschaffungsplanung.

2.10.3.3 Personalgewinnungsplanung

Es existieren grundsätzlich zwei Methoden zur Akquirierung, die Externe sowie die Interne. Bei der externen Variante kann durch unterschiedliche Maßnahmen neues Personal generiert werden. Dieses kann grundsätzlich durch professionelle Unterstützung bzw. Beauftragung durch Personalberater möglich sein oder durch eine Stellenausschreibung vorgenommen werden. Bei der internen Variante der Personalbeschaffung wird eine geeignete Mitarbeiterin oder Mitarbeiter durch Beförderung auf die erforderliche Stelle angeworben.

Die internen Personalbeschaffung meint die Rekrutierung des potenziellen Personals aus den eigenen Reihen d. h. über den sogenannten „internen Arbeitsmarkt“. Bei der externen Variante geht es um Neueinstellung von Personen, die bis dahin nicht der Unternehmung angehört haben.[1110]

2.10.3.4 Personalentwicklung

Die Personalentwicklung verfolgt das Ziel, Mitarbeiter oder Mitarbeitergruppen des Unternehmens bei der effizienten und erfolgreichen Bewältigung der Arbeitsaufträge bzw. dem Erreichen der Unternehmensziele durch geeignete Maßnahmen zu unterstützen. Damit umfasst die Personalentwicklung alle Maßnahmen der strategischen

[1110] Wirtschafts-Lexikon, 2006, Mag, S. 4455, Abschnitt 4. Personelle Maßnahmenplanung, Band 8.

Personalplanung, der Personalauswahl, der Aus-, Fort- und Weiterbildung sowie der Förderung und Beurteilung von Mitarbeitern. Im optimalen Fall leitet sich die strategische Personalplanung aus der Unternehmensstrategie ab und die Planungsparameter sind bekannt und fixiert.[1111]

2.10.3.5 Personalfreisetzung

Darunter ist die Verminderung des personellen Produktivitätspotenzials eines Unternehmens zu verstehen. Daneben wird der Begriff auch für personelle Einzelmaßnahmen verwendet, deren Ziel die Beendigung von Arbeitsverhältnissen ist. Veränderungen und Anpassungen organisatorischer Art sind fester Bestandteil eines kontinuierlich stattfindenden **Organisationsentwicklungsprozesses** in Unternehmen. Dabei bedeuten Personalanpassungsmaßnahmen immer eine **tiefgreifende Veränderung** für die betroffenen Mitarbeiter, aber auch für das Unternehmen in Gänze.[1112]

2.10.3.6 Datenschutzrechtliche Probleme bei der Personalplanung

Im Bereich der Personalbedarfsplanung ergeben sich datenschutzrechtlich keinerlei Probleme, da die dortigen Planungsergebnisse lediglich abstrakte Werte festlegen und sich nicht auf identifizierbare oder identifizierte natürliche Personen beziehen und daher regelmäßig keine personenbezogene Daten im Sinne von Art. 4 Nr. 1 DS-GVO sind.

Die interne Personalgewinnung, die Personaleinsatzplanung sowie die Personalentwicklungs- und Personalbedarfsplanung beschäftigen sich allerdings mit bereits vorhandenem Personal, sodass diese Bereiche der Personalplanung hier im Rahmen der Betrachtung der Einstellung und ihrer Vorbereitung außer Betracht bleiben können. Es bleiben nur die Probleme bei der externen Personalgewinnung zu betrachten. Klassisches Element der externen Personalgewinnung ist die Stellenausschreibung, sei es in Printmedien oder in Online-Jobbörsen.[1113]

1111 *Springer Gabler Verlag* (Hrsg.), Personalentwicklung, Gabler Wirtschaftslexikon, https://wirtschaftslexikon.gabler.de/definition/personalentwicklung-52604/version-330100.

1112 *Springer Gabler Verlag* (Hrsg.), Personalfreisetzung, Gabler Wirtschaftslexikon, https://wirtschaftslexikon.gabler.de/definition/personalfreisetzung-43403/version-266733.

1113 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Weth, S. 335, Rn. 6 und 7.

2.10.4 Stellenausschreibung

Die Stellenausschreibung ist die allgemeine Aufforderung an alle oder eine bestimmte Gruppe von Arbeitnehmern, sich für einen bestimmten Arbeitsplatz im Betrieb zu bewerben. Ein bestimmter Inhalt der Ausschreibung ist gesetzlich nicht festgelegt, jedoch muss gemäß dem Sinn und Zweck der Ausschreibung aus ihr hervorgehen, um welchen Arbeitsplatz es sich handelt und welche Anforderungen der Bewerber zu erfüllen hat. Schreibt der Arbeitgeber eine Stelle öffentlich oder innerhalb seines Betriebs aus, muss er die Regelungen der §§ 1, 7, 11 AGG[1114] beachten, die sicherstellen sollen, dass schon der erste Schritt eines Bewerbungsverfahrens diskriminierungsfrei erfolgt.[1115]

Die Stellenausschreibung soll den Bewerber dazu motivieren, personenbezogene Daten an den potenziellen Arbeitgeber zu übermitteln. Mit der Stellenausschreibung erhebt der Arbeitgeber also Daten, weil er sich durch sie personenbezogene Daten des Bewerbers verschafft.[1116]

Erheben von Daten ist eine Art der Verarbeitung (vgl. Art. 4 Nr. 2 DS-GVO). Hierzu ist zusätzlich Art. 88 DS-GVO (Datenverarbeitung im Beschäftigungskontext) einzubeziehen.

Abs.1 führt aus: „Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und

1114 AGG - Allgemeines Gleichbehandlungsgesetz.
1115 Thüsing, BGB § 611a Vertragstypische Pflichten beim Arbeitsvertrag, Rn. 2.
1116 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Weth, S. 335, Rn. 8 Abs. 1.

Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen."[1117]

Erwägungsgrund 155

Im Recht der Mitgliedstaaten oder in Kollektivvereinbarungen (einschließlich 'Betriebsvereinbarungen') können spezifische Vorschriften für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorgesehen werden, und zwar insbesondere Vorschriften über die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen, über die Verarbeitung dieser Daten für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses.[1118]

Gemäß § 26 Abs. 8 Satz 2 BDSG, gelten Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis als Beschäftigte.[1119] Den Begriff «Beschäftigtendaten» definiert die DS-GVO nicht. Vielmehr nimmt Art. 88 DS-GVO Bezug auf die Mitgliedstaatlichen Regelungen und ist akzessorisch zu diesen. In Deutschland gilt also die Definition des Beschäftigten aus § 26 Abs. 8 BDSG.[1120] Die Verarbeitung der personenbezogenen Daten der Stellenbewerber ist zulässig, wenn eine wirksame Einwilligung der Betroffenen vorliegt.[1121]

1117 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 88 Abs. 1 DSGVO.

1118 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 155 DSGVO.

1119 Bundesdatenschutzgesetz, § 26 Abs. 8 Satz 2 BDSG.

1120 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Forst, S. 1091, Rn. 13 Beschäftigtendaten Art. 88 DSGVO.

1121 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Weth, S. 336, Rn. 12 Satz 1.

2.10.5 Automatische Einzelentscheidungen

Die gesetzlichen Regelungen über automatisierte Entscheidungsfindung führen bislang eher ein Nischendasein. Mit dem technischen Fortschritt der künstlichen Intelligenz wird die praktische Bedeutung des Art. 22 DS-GVO zunehmen.[1122] Nach Art. 22 DS-GVO sind Entscheidungen mit rechtlichen Folgen oder erheblichen Beeinträchtigungen für die Betroffenen grundsätzlich unzulässig, soweit sie sich auf automatisierte Bewertungen von Persönlichkeitsmerkmalen stützen, ohne dass eine natürliche Person die entscheidungserheblichen Sachverhalte prüft und auf dieser Basis eigenständige Entscheidungen trifft.[1123]

2.10.6 Vorstellungsgespräch

Jeder Arbeitgeber ist bestrebt, in einem Einstellungsgespräch möglichst viele Informationen über den Bewerber in Erfahrung zu bringen. Jedoch darf er nicht jede beliebige Frage stellen. Seinem Informationsbedürfnis sind Grenzen gesetzt. Diese ergeben sich insbesondere aus dem BDSG, dem AGG, den GenDG, dem BZRG sowie aus dem allgemeinen Persönlichkeitsrecht und den daraus von der Rechtsprechung entwickelten Grundsätze zum Fragerecht des Arbeitgebers.[1124]

Nachfolgende Aufzählung führt die gängigsten Fragen bei Vorstellungsgesprächen auf, zulässige und nicht zulässige Fragen (kein Anspruch auf Vollständigkeit).

Uneingeschränkt zulässig sind:

- Fragen nach einer Schwerbehinderteneigenschaft
- Wehr-Ersatzdienstpflicht
- Künftig zu verbüßender Freiheitsstrafe
- Höhe des bisherigen Lohnes oder Gehalts
- Vorliegende Pfändung des Lohnes oder des Gehalts
- Gründe für einen Wechsel
- Ansteckende Krankheiten

1122 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Broy/Heinson, S. 383, Rn. 60 Satz 1.
1123 *Gola,* Handbuch Beschäftigtendatenschutz, 8. Aufl. 2019, S. 169, Rn. 588.
1124 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Weth, S. 359, Rn. 114.

- Alkoholabhängigkeit, sofern diese die auszuübende Tätigkeit tangiert (bspw. Kraftfahrer)

Nicht uneingeschränkt zulässig sind Fragen:

- Vorstrafen sofern keine Relevanz für die auszuübende Tätigkeit
- Politische Zugehörigkeit
- Religiöse Zugehörigkeit
- Zugehörigkeit zu einer Gewerkschaft
- Krankheiten, welche keinen Bezug zur auszuführenden Tätigkeit aufweisen
- Bevorstehende Heirat (oft an weibliche Bewerber gerichtet)
- Schwangerschaft (bestehende oder geplante, erneut in Abhängigkeit der Tätigkeit die angestrebt wird)

Die oben aufgeführten Fragen, zulässig oder nur eingeschränkt zulässig, sind in Abstimmung mit der aktuellen Rechtsprechung sowie den bestehenden Gesetzen anzuwenden. Hier sind insbesondere aber nicht abschließend der § 1 ff. AGG zu beachten.

Allgemeines **G**leichbehandlungs**g**esetz (**AGG**)

§ 1 Ziel des Gesetzes

„Ziel des Gesetzes ist, Benachteiligungen aus Gründen der Rasse oder wegen der ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität zu verhindern oder zu beseitigen.“

Alle Bewerberinnen und Bewerber müssen vorab über den Umfang der Erhebung der persönlichen Daten informiert werden. Zu diesem Zweck muss eine Datenschutzerklärung vorhanden sein, auf welche Bezug genommen werden kann. Darüber hinaus ist eine Einwilligung gemäß Art. 7 DS-GVO in Verbindung mit Erwägungsgrund 32, ebenso § 26 BDSG, zu beachten. Diese Einwilligung zur Nutzung der Daten muss vor dem entsprechenden Bewerbungsverfahren erteilt werden.

Personenbezogene Daten dürfen in der Regel auch ohne ausdrückliche Zustimmung verarbeitet werden, **sofern** diese dem Zwecke der **möglichen Aufnahme *eines* Beschäftigungsverhältnisses dient** und die Daten hierfür geeignet sind.

Ebenso muss im Vorfeld eines persönlichen Gesprächs die weitere Verarbeitung der eingereichten Unterlagen angesprochen werden. Dieses gilt uneingeschränkt für Online Bewerbungen, schriftlicher oder sonstigen Arten der Bewerbung. Bei Bewerbungen per

Videokonferenz aus einem Drittland ist vorab zu prüfen, wie es sich mit der Datenschutzrelevanz verhält. Hier ist insbesondere das Datenschutzabkommen mit den USA zu erwähnen (*Privacy Shield* und das *Safe Harbor Abkommen*[1125]).

Gespeicherte Daten sind in der Regel nach spätesten sechs Monaten zu entsorgen, es sei denn es wurde etwas anderes vereinbart. Unterlagen eines potenziellen Bewerbers oder Bewerberin sind bei nicht Einigung oder Befähigung nicht einfach durch den Müll zu entsorgen. Meist werden schriftliche Dokumente eingescannt und per E-Mail versandt. Dadurch werden diese Daten Bestandteil der „digitalen Kette". Einmal digital erfasste Daten durchlaufen bspw. ein geplantes Backup und werden dadurch mehrfach auf unterschiedlichen Datenträgern abgelegt.

Daten können sich in der Regel anschließend auf:

- Festplatten (bei Redundanz auf mehreren Platten),
- In Cloud Systemen,
- Auf den entsprechenden Geräten wie bspw. Smartphones, Tablet Computer, Notebooks oder auf privaten Geräten, welche im Homeoffice genutzt werden,
- Bei E-Mail Providern,
- USB-Sticks / mobile Festplatten,
- Im Speicher eines Scanners und oder Kopierers,

befinden.

Es muss gewährleistet sein, dass alle Daten entsprechend der Datenschutz-Grundverordnung richtig entsorgt und oder gelöscht werden. Es würde sich anbieten, papierbasierende Bewerbung im Anschluss an ein Bewerbungsverfahren zurück zu senden oder in Absprache mit dem Bewerber ordnungsgemäß zu vernichten.

1125 N. *Jung,* Abolition of the Safe Harbour Agreement: Legal situation and alternatives, http://hdl.handle.net/10419/148370.

2.10.7 Personalakten

Grundsätzlich ist unter einer Personalakte jede Sammlung von Urkunden und Vorgängen, die persönlich und arbeitsrechtsrelevante Verhältnisse eines Arbeitnehmers betreffen und in einem inneren Zusammenhang mit dem Arbeitsverhältnis stehen, zu verstehen.[1126] Unter den Begriff der Personalakte fallen auch die in einer elektronischen Datenbank gespeicherten Personaldaten, auf die der Arbeitgeber zum Zwecke der Personalinformation oder Personalmaßnahme zurückgreifen kann.[1127]

Das BAG unterscheidet zwischen dem materiellen und dem formellen Personalaktenbegriff.[1128] Unter formellen Personalakten sind diejenigen Schriftstücke und Dokumente zu verstehen, die der Arbeitgeber als Personalakte führt oder diesen als Bei-, Neben- oder Sonderakten zuordnet. Solche Aktenbestände sind äußerlich erkennbar Ordnern, Heftern oder Blattsammlungen geführt, entsprechend gekennzeichnet und nach der Art der Registrierung oder Aufbewahrung als zueinander gehörig bestimmbar.[1129] Unter der Personalakte im materiellen Sinn ist jede Sammlung von Urkunden und Vorgängen zu verstehen, die die persönlichen und dienstlichen Verhältnisse des Arbeitnehmers betreffen und in einem inneren Zusammenhang mit dem Arbeitsverhältnis stehen.[1130]

Die Personalakte soll ein möglichst vollständiges, wahrheitsgemäßes und sorgfältiges Bild über die persönlichen und dienstlichen Verhältnisse des Arbeitnehmers geben. Es ist unerheblich, wie der Arbeitgeber einen Vorgang, der zur Personalakte gehört, bezeichnet und wo und wie er ihn führt und aufbewahrt. Allein entscheidend ist der Inhalt des Vorgangs. Erfüllt dieser die begrifflichen Merkmale einer Personalakte, ist der Vorgang als Personalakte zu qualifizieren.[1131]

1126 *Auffarth et al.,* Betriebsverfassungsgesetz, 29. Aufl. 2018, S. 1402, Abs. 1, Rn. 3 - § 83 BetrVG. Vgl. ebenfalls BAG 19.7.2012 - 2 AZR 782 / 11.

1127 *Auffarth et al.,* Betriebsverfassungsgesetz, 29. Aufl. 2018, S. 1402, Rn. 3 - § 83 BetrVG. Vgl. ebenfalls Nebeling / Lankes DB 2017, 2542.

1128 Bundesarbeitsgericht - BAG, 4 AZR 214/78 http://www.prinz.law/urteile/BAG_4_AZR_214-78, 1 - 12.

1129 Bundesarbeitsgericht - BAG, 16. November 2010 – 9 AZR 573/09 https://juris.bundesarbeitsgericht.de/zweitesformat/bag/2015/2015-03-23/9_AZR_573-09.pdf.

1130 Bundesarbeitsgericht - BAG, 4 AZR 214/78 http://www.prinz.law/urteile/BAG_4_AZR_214-78, 1 - 12.

1131 Bundesarbeitsgericht - BAG, 4 AZR 214/78 http://www.prinz.law/urteile/BAG_4_AZR_214-78, 1 - 12 (Seite 7).

Ausschlaggebend für die Beurteilung, ob ein Schriftstück zur Personalakte zählt, ist der materielle Personalaktenbegriff, weil es nicht darauf ankommt, ob der Arbeitgeber Unterlagen als „Personalakte“ bezeichnet.[1132]

Außerhalb des Beamtenrechts (vgl. § 106 Absatz 1 Satz 1 BBG) gibt es, abgesehen von einigen gesetzlichen Vorschriften (wie etwa § 257 HGB, § 147 AO, § 41 Abs. 1 Satz 9 EstG), keine gesetzlichen Bestimmungen, die den Arbeitgeber verpflichtet, Personalakten zu führen.[1133] Aufgrund seiner betrieblichen Leistungs- und Organisationsmacht ist der Arbeitgeber jedoch berechtigt, Personalakten zu führen.[1134]

Im Datenschutz wird der Personalakte darüber hinaus ein gewisser **Sonderstatus** zugestanden, denn in der Regel beziehen sich entsprechende Gesetze auf eine automatisierte Datenerhebung – also digitalisierte und elektronisch hinterlegte Daten. Das BDSG führt hierzu explizit aus, dass **nicht nur eine elektronische Personalakte unter den Datenschutz fällt, sondern im Besonderen auch jede nicht automatisierte Papierakte** (vgl. § 32 Absatz 2 BDSG).[1135]

2.10.7.1 Zulässiger Inhalt

In eine Personalakte dürfen nur die für das Arbeitsverhältnis **erforderlichen Daten** unter **Abwägung** der **beiderseitigen Interessen** aufgenommen werden.[1136] Unbeachtlich ist dabei, wann die Unterlagen entstanden und zum Arbeitgeber gelangt sind.[1137] In einer Personalakte dürfen alle Unterlagen von der **Bewerbung**, dem **Abschluss** des **Arbeitsvertrages**, der **Durchführung des Arbeitsverhältnisses** bis hin zur **Beendigung** und **Abwicklung** des Arbeitsverhältnisses aufgenommen werden.[1138]

2.10.7.2 Unzulässiger Inhalt

Nicht zur Personalakte gehören auch die **Prozessakten über einen Rechtsstreit** zwischen Arbeitgeber und Arbeitnehmer, weil es dem Prozessrecht widerspricht, seinem

---

1132 *Simitis/Dammann/Arendt* (Hrsg.), Bundesdatenschutzgesetz, § 32 BDSG, Rn. 109.
1133 *Simitis/Dammann/Arendt* (Hrsg.), Bundesdatenschutzgesetz, Seifert, § 32, Rn. 111.
1134 *Kiel/Lunk/Oetker* (Hrsg.), Münchener Handbuch zum Arbeitsrecht Individualarbeitsrecht, Reichold, § 87, Rn. 6.
1135
1136 *Kiel/Lunk/Oetker* (Hrsg.), Münchener Handbuch zum Arbeitsrecht Individualarbeitsrecht, § 87 Rn. 8 ArbR.
1137 *Kiel/Lunk/Oetker* (Hrsg.), Münchener Handbuch zum Arbeitsrecht Individualarbeitsrecht, § 87 Rn. 8 ArbR.
1138 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Breyer, S. 387, Rn. 5, Teil B.

Gegner Einsicht in die Prozessakten zu gewähren.[1139] Nicht zum Inhalt einer Personalakte gehören ebenfalls die **Aufzeichnungen und Unterlagen des Betriebsarztes** die wegen der ärztlichen Schweigepflicht nach § 8 Abs. 1 Satz 3 ASiG[1140] dem Arbeitgeber nicht zugänglich sind.[1141] Weiterhin zählen **betriebliche Unterlagen**, wie etwa Schichtpläne, Personal-, Lohn- und Gehaltslisten, in denen der Arbeitnehmer nur namentlich aufgeführt wird, nicht zu den Personalakten, da diese Unterlagen auch Daten über andere Arbeitnehmer enthalten.[1142] Schließlich gehören auch die **persönlichen Aufzeichnungen** des Arbeitgebers, wie Zeugnisentwürfe, Ideenskizzen und Planungsunterlagen für Personalentscheidungen nicht zur Personalakte.[1143]

2.10.7.3 Vollständigkeit und Richtigkeit

Nach dem **Prinzip der Vollständigkeit**, soll die Personalakte möglichst vollständig und lückenlos über die Person des Arbeitnehmers und seine Laufbahn Aufschluss geben.[1144] Zu beachten ist allerdings das Prinzip der Richtigkeit der Personalakte. Hiernach hat der Arbeitgeber dafür Sorge zu tragen, dass die Personalakte ein möglichst **zutreffendes Bild** von der Person, der Tätigkeit und den Leistungen des Arbeitnehmers vermittelt.[1145] Der Arbeitnehmer hat deswegen einen Anspruch darauf, dass die in seine Personalakte aufgenommenen Angaben **zutreffend und sachlich richtig** sind.[1146]

Das Prinzip der Richtigkeit gilt sowohl für Tatsachenbehauptungen als auch für Werturteile.[1147] Ausfluss dieses Prinzips ist das Recht des Arbeitnehmers, die Entfernung unrichtiger Angaben aus der Personalakte verlangen zu können.[1148] Allerdings hat der Arbeitgeber weiterhin das Recht, für den Arbeitnehmer nachteilige Unterlagen in die

1139 *Kiel/Lunk/Oetker* (Hrsg.), Münchener Handbuch zum Arbeitsrecht Individualarbeitsrecht, Reichold, § 87 Rn. 5.
1140 Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit, ASiG, § 8 Abs. 1 Satz 3, Schweigepflicht).
1141 *Fitting/Auffarth/Kaiser,* Betriebsverfassungsgesetz, 30. Aufl. 2020, § 83, Rn. 6 BetrVG.
1142 *Fitting/Auffarth/Kaiser,* Betriebsverfassungsgesetz, 30. Aufl. 2020, § 83, Rn. 6 BetrVG.
1143 *Eisemann,* Personalbuch 2019, Personalakte, Rn. 6.
1144 Bundesarbeitsgericht - BAG, 1 AZR 322/71 (25.04.1972).
1145 *Kiel/Lunk/Oetker* (Hrsg.), Münchener Handbuch zum Arbeitsrecht Individualarbeitsrecht, § 87 Rn. 12.
1146 *Gola/Wronka,* Handbuch Arbeitnehmerdatenschutz, 6. Aufl. 2013, Rn. 125.
1147 *Gola/Wronka,* Handbuch Arbeitnehmerdatenschutz, 6. Aufl. 2013, Rn. 123.
1148 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, S. 389, Rn. 8.

Personalakte aufzunehmen, wenn dies erforderlich ist, um ein klares Bild über die Person des Arbeitnehmers zu erhalten.[1149]

2.10.7.4 Vertraulichkeit

Der Arbeitgeber hat die Personalakte seiner Arbeitnehmer sorgfältig zu verwahren und darauf zu achten, dass die Personalakten nicht allgemein zugänglich sind. Er muss die Personalakten vertraulich behandeln oder für die vertrauliche Behandlung durch die Sachbearbeiter Sorge tragen und den Kreis der mit Personalakten befassten Beschäftigten möglichst eng halten.[1150] Besonders sensible Daten (Angaben über den körperlichen, geistigen und gesundheitlichen Zustand und allgemeine Aussagen über die Persönlichkeit des Arbeitnehmers) bedürfen eines verstärkten Schutzes.[1151]

2.10.7.5 Einsichtsrecht

Nach § 83 Abs. 1 Satz 1 BetrVG hat jeder Arbeitnehmer das Recht, in **die über ihn** geführten Personalakten Einsicht zu nehmen (für leitende Angestellte gilt § 26 Abs. 2 Satz 1 SpAuG[1152]). Dieses Einsichtsrecht steht allen Arbeitnehmern zu, auch den Auszubildenden und bezieht sich auf die Personalakte im **materiellen Sinn**.[1153]

Beim Datenschutz gilt es zu berücksichtigen, dass nur **Befugte Personen** Zugriff auf die personenbezogenen Daten haben dürfen. Sie müssen entsprechend vor dem unbefugten Zugriff Dritter bewahrt werden. Das gilt analog auch für jede Personalakte. Im öffentlichen Dienst finden sich entsprechende Vorschriften zum Datenschutz in der Personalabteilung u.a. im Bundesbeamtengesetz (§§ 106 bis 115 BBG).

Wesentliche Bestimmungen diesbezüglich sind:

- Gemäß Datenschutz gilt: Die Personalakte darf der Vorgesetzte ebenfalls nicht **beliebig** einsehen.

1149 *Kiel/Lunk/Oetker* (Hrsg.), Münchener Handbuch zum Arbeitsrecht Individualarbeitsrecht, Reichold, § 87, Rn. 12.

1150 *Rolfs, Christian/Witschen, Stefan*, Bürgerliches Gesetzbuch 2002, Anmerkung zu BAG 9 AZR 271/06 (EZA: BGB 2002, § 611 Persönlichkeitsrecht Nr. 4), in Entscheidungssammlung zum Arbeitsrecht 2007, 11.

1151 *Rolfs/Witschen* Entscheidungssammlung zum Arbeitsrecht 2007, 11.

1152 Gesetz über Sprecherausschüsse der leitenden Angestellten.

1153 *Kiel/Lunk/Oetker* (Hrsg.), Münchener Handbuch zum Arbeitsrecht Individualarbeitsrecht, Reichold, § 87 Rn. 18.

- Die Personalakte ist gemäß Datenschutz **vertraulich** zu behandeln.[1154]
- Sie muss ausreichend vor **unbefugter Einsichtnahme** gesichert sein[1155]
- Der Kreis der Einsichtsberechtigten muss nach einem Urteil des Bundesarbeitsgerichts vom 15. Juli 1987 vom Vorgesetzten möglichst klein gehalten werden.[1156]
- Auch bei Berechtigung ist die Einsicht in die Personalakte jedoch nur dann zulässig, wenn dies zum Zwecke der Personalverwaltung bzw. einer Personalangelegenheit erfolgt. Also auch Personalverwalter dürfen nicht beliebig Einsicht nehmen. Und auch der Vorgesetzte darf sich nicht einfach beliebig der Personalakten bedienen.[1157]

2.10.7.6 Entfernungsanspruch

Bei unrichtigen oder sonst unzulässigen Personalaktenunterlagen, die geeignet sind, den Arbeitnehmer in seiner Rechtsstellung und in seinem beruflichen Fortkommen zu beeinträchtigen, hat der Arbeitnehmer einen Anspruch auf Berichtigung oder Entfernung dieser Unterlagen.[1158]

2.10.8 Videoüberwachung

Der Einsatz von Videokameras am Arbeitsplatz befindet sich oftmals in einer juristischen Grauzone. Regelmäßig steht dem Einsatz einer Videokamera das allgemeine Persönlichkeitsrecht der Arbeitnehmer entgegen, in welches nicht rechtswidrig eingegriffen werden darf. In der Praxis besteht in vielen Fällen keine Rechtssicherheit darüber, ob die Videoüberwachung rechtmäßig erfolgt.[1159]

1154 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 1 DSGVO, vgl. hierzu auch Erwägungsgrund 1 DSGVO.

1155 *Piltz,* BDSG, 2018, vgl. § 9 BDSG, S. 67.

1156 Bundearbeitsgericht, 15.07.1987 – 5 AZR 215/86 http://www.prinz.law/urteile/BAG_5_AZR_215-86.

1157 *VFR Verlag für Rechtsjournalismus GmbH*, Wer darf die Personalakte laut Datenschutz einsehen?, https://www.datenschutz.org/personalakte/.

1158 Bundesarbeitsgericht - BAG, 14. Juni 1983 https://www.prinz.law/urteile/BAG_5_AZR_101-84.

1159 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Byers, S. 475, Rn. 2.

Die Videoüberwachung wird auch nach dem 25. Mai 2018 sowohl für die Aufsichtsbehörden als auch für die Betreiber entsprechender Anlagen ein Thema mit erheblicher praktischer Relevanz bleiben. Die DS-GVO selbst enthält keine spezifische Regelung zur Videoüberwachung. Somit ist nicht klar, in welchem Umfang die bisherigen datenschutzrechtlichen Bewertungen in der Praxis beibehalten werden können. Der ab dem 25. Mai 2018 ebenfalls in Kraft tretende § 4 des Bundesdatenschutzgesetzes (BDSG-neu, vgl. Art. 1 DSAnpUG-EU) enthält zwar eine Regelung zur Videoüberwachung öffentlich zugänglicher Räume. Ob und in welchem Umfang diese Regelung aufgrund des Anwendungsvorrangs der DS-GVO angewendet werden kann, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.[1160]

2.10.8.1 Begriff der Videoüberwachung

Bei der Bestimmung des Begriffs der Videoüberwachung am Arbeitsplatz lässt sich auf die Definition der Überwachung nach § 87 Abs. 1 Nr. 6 BetrVG abstellen.[1161] § 87 Abs. 1 Nr. 6 BetrVG regelt das Mitbestimmungsrecht des Betriebsrats bei der technischen Überwachung eines Mitarbeiters. Darunter fällt zweifelsfrei auch die Videoüberwachung. Daraus ergibt sich, dass eine Videoüberwachung des Arbeitnehmers begrifflich immer dann vorliegt, wenn auch das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG eröffnet wäre.[1162]

2.10.8.2 Rechtsgrundlage für die Videoüberwachung

Die schlichte Anwendung von Art. 9 DS-GVO ohne entsprechende Tatbestandsreduktion bedeutet, dass die Zulässigkeit der Videoüberwachung neben Art. 6 auch an Art. 9 DS-GVO zu messen ist.[1163] Es stellt sich die daher die Frage, inwieweit Ausnahmetatbestände einschlägig sind bzw. ob eine Öffnungsklausel für die Regelung durch den nationalen Gesetzgeber besteht.[1164]

1160 *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz* 17.12.2018, 1 (S. 1).
1161 *Byers,* Mitarbeiterkontrollen, 2016, S. 11.
1162 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Byers, S. 476, Rn. 4 (Teil B).
1163 Amtsblatt der Europäischen Union 04.05.2016 (Vgl. Erwägungsgrund 51 Satz 5 DSGVO).
1164 *Wiebke Reuter LL.M.* ZD - Zeitschrift für Datenschutz, 564 (S. 566, Abs. 1 Satz 2, Rechtsgrundlage für die Videoüberwachung).

Vorschriften zur allgemeinen Videoüberwachung für öffentliche Stellen finden sich sowohl in § 4 BDSG als auch in allen Landesdatenschutzgesetzen.[1165] Soweit § 4 BDSG nach dem Wortlaut und der gesetzgeberischen Intention auch die Datenverarbeitung durch nicht-öffentliche Stellen zu privaten Zwecken erfassen soll, ist die Vorschrift europarechtswidrig, weil es an einer Regelungsbefugnis des deutschen Gesetzgebers fehlt.[1166] Die Zulässigkeit der Videoüberwachung durch private Stellen zu eigenen Zwecken richtet sich in Bezug auf die „einfachen" personenbezogenen Daten nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO. [1167]

Wesentlich konkreter und detaillierter als die alte Regelung sind allerdings die Anforderungen an die Transparenz.[1168] Artikel 13 DS-GVO enthält einen langen Katalog von Pflichtinformationen, die bereitzustellen sind. Diese reichen von den Kontaktdaten der oder des Verantwortlichen[1169] und ggf. der oder des Datenschutzbeauftragten über die Interessen, die Zwecke und die Rechtsgrundlage der Datenverarbeitung bis hin zur Speicherdauer und zu Betroffenenrechten.

Die DS-GVO ermöglicht in Art. 9 Abs. 2 DS-GVO die Verarbeitung sensibler Daten i.R.d. Videoüberwachung. Ob darüber hinaus, etwa durch die Reduktion des Tatbestands von Art. 9 DS-GVO mit Hilfe des Merkmals der Auswertungsabsicht, Ausnahmen für die Videoüberwachung bestehen oder geschaffen werden, kann nur auf europäischer Ebene entschieden werden. Art. 9 Abs. 2 lit. g DS-GVO sieht eine Öffnungsklausel vor, wenn die Verarbeitung sensibler Daten aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist. Private Interessen genügen diesem nicht.[1170]

2.10.8.3 Kenntlichmachung

Eine offene Videoüberwachung ist durch geeignete Maßnahmen kenntlich zu machen. Es wird allerdings weder nach der DS-GVO noch nach dem BDSG festgelegt, auf welche Art und Weise die Kenntlichmachung zu erfolgen hat. Es ist allerdings sicherzustellen,

---

1165 *Wiebke Reuter LL.M.* ZD - Zeitschrift für Datenschutz, 564 (vgl. Aufzählung Quellennummer. 22, S. 566).
1166 *Taeger/Gabel* (Hrsg.), DSGVO - BDSG Kommentar, § 4, Rn. 35 ff. BDSG.
1167 *Wiebke Reuter LL.M.* ZD - Zeitschrift für Datenschutz, 564 (S. 566, Abs. 2, Rechtsgrundlage für die Videoüberwachung).
1168 *Paal u. a.* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Art. 12 ff. DSGVO.
1169 *Bäcker,* Datenschutz-Grundverordnung, Bäcker, S. 355, Rn. 22 ff.
1170 *Wiebke Reuter LL.M.* ZD - Zeitschrift für Datenschutz, 564 (S. 566, Öffnungsklausel Art. 9 DSGVO sowie S. 569).

dass die Videoüberwachung kenntlich gemacht wird.[1171] In der Regel werden Aufkleber und / oder Schilder verwendet, auf denen ein weißes Video-Kamerasymbol auf blauem Hintergrund gezeigt wird (Piktogramm). Diese Symbolik ermöglicht das Ansprechen eines internationales Publikums, ohne in allen gängigen Sprachen eine Erklärung liefern zu müssen.

Neben der Rechtmäßigkeit der Verarbeitung fordert die DS-GVO in Art. 5 Abs. 1 lit. a ferner, dass die personenbezogenen Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen. Mit dieser Regelung sowie den sich aus Art. 12 ff. DS-GVO ergebenden Anforderungen, sind die Transparenzpflichten stark angestiegen. Aus den Informationspflichten nach Art. 13 Abs. 1 und 2 DS-GVO ergeben sich folgende Mindestanforderungen:[1172]

- Umstand der Beobachtung – Piktogramm, Kamerasymbol.
- Identität des für die Videoüberwachung Verantwortlichen – Name einschl. Kontaktdaten (Art. 13 Abs. 1 lit. a DS-GVO). Videoüberwachung nach der Datenschutzgrundverordnung Stand: 17.12.2018
- Kontaktdaten des betrieblichen Datenschutzbeauftragten – soweit benannt, dann aber zwingend (Art. 13 Abs. 1 lit. b DS-GVO).
- Verarbeitungszwecke und Rechtsgrundlage in Schlagworten (Art. 13 Abs. 1 lit. c DS-GVO).
- Angabe des berechtigten Interesses – soweit die Verarbeitung auf Art. 6 Abs. 1 S. 1 lit. f DS-GVO beruht (Art. 13 Abs. 1 lit. d DS-GVO).
- Dauer der Speicherung (Art. 13 Abs. 2 lit. a DS-GVO).
- Hinweis auf Zugang zu den weiteren Pflichtinformationen gem. Art. 13 Abs. 1 und 2 DS-GVO (wie Auskunftsrecht, Beschwerderecht, ggf. Empfänger der Daten).

1171 *Körffer et al.,* Bundesdatenschutzgesetz, 10. Aufl. 2010, S, 228, Rn. 25, § 6b BDSG a.F.

1172 *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz* 17.12.2018, 1 (S. 2 Transparenzanforderungen und Hinweisbeschilderung).

Es ist sicherzustellen, dass die Videoüberwachung bereits bei Betreten des überwachten Raumes erkennbar ist.[1173] Dem Arbeitgeber ist allerdings nicht zu empfehlen, sich ausschließlich auf die sichtbare Kamerainstallation als Mittel der Kenntlichmachung zu verlassen. Unter Umständen kann das Kameragerät zu klein sein und mit anderen Geräten – wie bspw. Rauchmeldern – verwechselt werden, sodass der Arbeitnehmer die Überwachung als solche nicht identifiziert.[1174]

2.10.8.4 Verdeckte Videoüberwachung

Die Zulässigkeit einer verdeckten Videoüberwachung am Arbeitsplatz wurde in Rechtsprechung und Literatur schon nach dem bisherigen BDSG a.F. sehr kritisch beurteilt. Aufgrund der starken Eingriffsintensität sollte nach Auffassung der bisherigen Rechtsprechung und in weiten Teilen der Literatur eine heimliche Überwachung grundsätzlich nur in sehr engen Ausnahmefällen möglich sein.[1175] Danach war Zulässigkeitsvoraussetzung für einen regelmäßigen Einsatz heimlicher Kameras, dass der konkrete Verdacht einer strafbaren Handlung zulasten des Arbeitgebers bestand, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft waren und die verdeckte Videoüberwachung praktisch das einzige verbleibende Mittel darstellte und insgesamt nicht unverhältnismäßig war.[1176]

Die DS-GVO und das neue BDSG sehen nun allerdings umfangreiche Transparenz- und Informationspflichten für Arbeitgeber vor, die einer Rechtmäßigkeit von heimlichen Videoüberwachungen entgegenstehen. So wird in der Literatur vertreten, dass der **Transparenzgrundsatz** des Art. 5 Abs. 1 lit. a DS-GVO eine heimliche Verarbeitung personenbezogener Daten künftig komplett ausschließen würde.[1177] Dies würde zu einem generellen Verbot einer verdeckten Videoüberwachung führen, da im Rahmen einer heimlichen Überwachung zwangsläufig personenbezogene Daten ohne Kenntnis der

---

1173 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Byers, S. 479, Rn. 20.

1174 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Byers, S. 480, Rn. 20.

1175 *Otto, Hansjörg*, BetrVG 1972 § 87: Anmerkung zu BAG 2 AZR 51/02 (AP: BetrVG 1972 § 87 Überwachung, Nr. 36), in Nachschlagewerk des Bundesarbeitsgerichts : AP, arbeitsrechtliche Praxis ; die Rechtsprechung des Bundesarbeitsgerichts und die arbeitsrechtlich bedeutsamen Entscheidungen anderer Gerichte mit erläuternden Hinweisen ; Wiedergabe der Leitsätze und Fundstellennachweise ; Kurzausgabe 2005, 87.

1176 Sächsisches Landesarbeitsgericht, 12.06.2003 – 2 SA 790/02.

1177 *Bäcker,* Datenschutz-Grundverordnung, Herbst, S. 198, Art. 5, Rn. 18, (Var. 3) DSGVO.

betroffenen Arbeitnehmer erhoben werden.[1178] Die DS-GVO verlangt eine Abwägung im konkreten Einzelfall sowohl im Hinblick auf die Interessen der Verantwortlichen bzw. Dritten als auch der Betroffenen. Ein bloßes Abstellen auf abstrakte oder auf vergleichbare Fälle ohne Betrachtung des Einzelfalls genügt den Anforderungen der DS-GVO daher nicht.[1179]

2.10.8.5 Beschäftigtendatenschutz

Im Beschäftigtendatenschutz können die dargelegten Grundsätze grundsätzlich weiterhin angewandt werden, vgl. § 26 BDSG n.F., Art. 88 Abs. 1 DS-GVO. Daher wird im Bereich der Videoüberwachung von Beschäftigten die ständige Rechtsprechung des Bundesarbeitsgerichts wie bisher zur Anwendung gelangen können. Die Interessenabwägung wird dabei an den Anforderungen des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zu messen sein.[1180]

Fraglich ist, inwieweit eine verdeckte Videoüberwachung von Beschäftigten zulässig bleibt. Insoweit ist es angemessen Einschränkungen der Transparenzverpflichtung im Beschäftigtendatenschutz zuzulassen. § 26 Abs. 1 BDSG-neu macht von der Öffnungsklausel des Art. 88 Abs. 1 DS-GVO Gebrauch, sodass grundsätzlich die bislang bestehende deutsche Rechtslage für die Verarbeitung von Beschäftigtendaten beibehalten wird. Ergänzend wird jedoch der Verantwortliche nach § 26 BDSG-neu verpflichtet, die Grundlagen der Datenverarbeitung nach Art. 5 DS-GVO einzuhalten.[1181]

2.10.8.6 Erforderlichkeit des Einsatzes von Videokameras

Die Videoüberwachung an einem Arbeitsplatz kann nur **rechtmäßig** erfolgen, wenn sie **erforderlich** ist. Von einer Erforderlichkeit des Überwachungsmittels ist dann auszugehen, wenn mit der Videoüberwachung der Überwachungszweck überhaupt erreicht werden kann und zugleich kein anderes **und milderes Mittel existiert**, mit dem sich der Zweck genauso effizient erreichen lässt.[1182]

1178 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Byers, S. 482 / 483, Rn. 26a.

1179 *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz* 17.12.2018, 1 (S. 2, Inhaltliche Voraussetzungen für eine Videoanlage).

1180 *Lachenmann* ZD - Zeitschrift für Datenschutz, 407 (S. 410 Abschnitt 2).

1181 *Lachenmann* ZD - Zeitschrift für Datenschutz, 407 (S. 411 Abs. 1).

1182 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Byers, S. 486, Rn. 32.

So kann z.B. eine heimliche Videoüberwachung ein **untaugliches Überwachungsmittel** darstellen, wenn der Kameraeinsatz **zur reinen Abschreckung** erfolgt. Damit der Präventionszweck erreicht werden kann, ist gerade die Sichtbarkeit der Videokamera notwendig.[1183] Die Zulässigkeit der verdeckten Videoüberwachung würde in solchen Fällen bereits an der **Schwelle der Erforderlichkeit** scheitern.[1184]

Aus den dargelegten Gründen ist es nicht möglich generell festzustellen, welche Überwachungsmittel als milder und damit erforderlich einzustufen sind. Vielmehr sind die Effizienz sowie Eingriffsintensität einer Videoüberwachung im konkreten Einzelfall festzustellen.[1185]

2.10.8.7 Geldbußen

Im Falle einer unzulässigen Videoüberwachung kommt gem. Art. 83 Abs. 1, Abs. 5 lit. a das nach der DS-GVO höchstmögliche Bußgeld in Höhe von bis zu 20 Mio. EUR „oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs“ in Betracht. Die maximal mögliche Bußgeldhöhe erscheint geboten, weil es einer unzulässigen Videoüberwachung an der Rechtmäßigkeit der grundsätzlich verbotenen Verarbeitung personenbezogener Daten mangelt. Ohne die Rechtmäßigkeit liegt ein unerlaubter schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung vor. Da die Informationspflichten bei der Videoüberwachung nach BDSG der Auffassung der DSK nach nicht in Einklang mit denen nach Art. 12 ff. sind, ist nicht auszuschließen, dass dem Rechtsanwender in Deutschland bei ausschließlicher Einhaltung des BDSG eine Geldbuße droht.[1186] Wegen des jedenfalls aus Sicht der deutschen Aufsicht bestehenden **Normenkonflikts** zwischen **DS-GVO** und **BDSG** wird die Praxis in eine unangenehme Situation mit möglicherweise teuren **Rechtsfolgen** gedrängt. Dass die auch von der Kommission bei der Notifizierung des BDSG unbeanstandete Nutzung der Öffnungsklauseln aus Art. 5 und 23 in § 4 BDSG tatsächlich europarechtswidrig ist, erscheint schon mit Blick auf deren weite Formulierung äußerst fraglich. Für die Praxis bleibt zu hoffen, dass diese

1183 *Simitis/Dammann/Arendt* (Hrsg.), Bundesdatenschutzgesetz, vgl. § 6b, Rn. 56 BDSG.
1184 *Weth u. a.* (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Byers, S. 486, Rn. 33.
1185 *Byers,* Mitarbeiterkontrollen, 2016, S. 92.
1186 *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz* 17.12.2018, 1 (S. 3, Abschnitt Konsequenz).

Meinungsverschiedenheit zwischen behördlicher Aufsicht und Gesetzgeber nicht anhand eines Bußgeldes auf dem Rücken der Betroffenen ausgetragen wird. Falls doch, wäre in diesem Fall eine Amtspflichtverletzung der Datenschutzaufsicht wegen unzulässiger Nichtanwendung des BDSG zu erwägen.[1187]

2.11 Datenschutzerklärung

Betreiber und oder Anbieter einer Webseite sind nach den Art. 12, 13 und 14 der DS-GVO zu prüfen, zu erstellen und auf Inhalt anzupassen. Art. 12 DS-GVO sieht unter anderem vor, dass alle notwendigen Informationen: „[…] in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln […]"[1188] sind. Dieses hört sich erst einmal einfach und sinnvoll an, muss aber bei der Gestaltung unbedingt Berücksichtigung finden. Nicht alle Besucher einer Webseite sind juristisch ausgebildet. Art. 13 DS-GVO wird in Bezug auf die Erhebung personenbezogener Daten schon konkreter. In dieser werden Anforderungen an die Informationspflicht bei der Erhebung von personenbezogenen Daten aufgezeigt.

Artikel 13

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a. den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
b. gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

1187 *Atztert/Buchmann/Dietze, Lars, Heidelberger Kommentar,* DSGVO/BDSG, Heidelberger Kommentar, Position 11654 von 87533, Rn. 36 (Geldbußen).

1188 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), vgl. Art. 12 DSGVO.

c. die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
d. wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
e. gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
f. gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a. die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
b. das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
c. wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
d. das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
e. ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte und

f. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.[1189]

Auf Grundlage des Art. 13 DS-GVO hat die Datenschutzerklärung aufzubauen, ergänzt um die entsprechenden Anforderungen an das jeweilige Gewerbe. Ausschlaggebend ist nicht die Größe eines Unternehmens, sondern der Umstand, dass personenbezogene Daten betroffener Personen verarbeitet werden. Dieses gilt insbesondere aber nicht abschließend für die Betreibung einer Homepage. Zum Thema Datenschutzerklärung auf einer Homepage, befindet sich ein Muster im Anhang. Diese muss entsprechend angepasst und überprüft werden.

Das **T**ele**m**edien**g**esetz gilt nach § 1 Abs. 1 für alle elektronischen Informations- und Kommunikationsdienste, soweit diese nicht dem Telekommunikationsgesetz oder dem Rundfunkstaatsvertrag unterstehen. Es findet auf alle Anbieter einschließlich der öffentlichen Stellen Anwendung.[1190] Als Anbieter im Sinne des **TMG** versteht man unter anderem auch juristische Personen (meist Unternehmen), die eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln, ob privat oder zur geschäftsmäßigen Nutzung. So ist **jede Website ein Telemedium** und **jeder Betreiber** ein **Dienstanbieter**. Nutzer nach dem Telemediengesetz ist jede natürliche

1189 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), Art. 13 DSGVO.

1190 *Spindler/Schmitz/Liesching,* Telemediengesetz mit Netzwerkdurchsetzungsgesetz; Kommentar, 2. Aufl. 2018, Spindler, § 1 Abs. 1 TMG, S.9.

oder juristische Person, die Telemedien nutzt, insbesondere zur Erlangung von Informationen.

Der Datenschutz ist im Telemediengesetz in den §§ 11 - 15a TMG geregelt. Anknüpfungspunkt dieser Vorschriften ist dabei der Schutz personenbezogener Daten bei der Erhebung und Verwendung (d.h. Verarbeitung und Nutzung) durch Dienstanbieter.[1191]

Grundsätzlich werden mitgliedstaatliche datenschutzrechtliche Regelungen aufgrund des **Anwendungsvorrangs der DS-GVO**[1192] durch diese verdrängt, wenn es keine spezifischen Regelungen gibt, die ein Fortbestehen bereits existierender Regelungen anordnen oder Öffnungsklauseln Spielräume zur mitgliedstaatlichen Ausgestaltung offen lassen beziehungsweise vorgeben.[1193]

Gemäß der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder sind die §§ 12, 13, 15 TMG (Grundsätze des Datenschutzes, Pflichten des Dienstanbieters, Nutzungsdaten) nicht mehr anwendbar. Zu diesem Schluss kommt der Bundesgerichtshof in seinem Urteil von 5. Oktober 2017.[1194]

Die im Anhang befindlichen Abbildungen zeigen ein Muster zur Datenschutzerklärung[1195]. Diese sollte in jedem Fall auf die entsprechenden Anforderungen angepasst oder durch zu Hilfenahme professionelle Unterstützung erstellt werden.

1191 *Konferenz der unabhängigen Datenschutzaufsichtsbehörden*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien März 2019.

1192 *Spindler/Schmitz/Liesching,* Telemediengesetz mit Netzwerkdurchsetzungsgesetz; Kommentar, 2. Aufl. 2018, Schmitz, S. 397, Rn. 9 Satz 1, vgl. auch Gola DSGVO Art. 6 Rn. 30, Art. 95 Rn. 18 f.

1193 *Konferenz der unabhängigen Datenschutzaufsichtsbehörden,* Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien.

1194 BGH - Bundesgerichtshof, Urteil v. 5.10.2017, I ZR 7/16 (erhältlich in juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=80132&pos=0&anz=1), I ZR 7/16.

1195 *VFR Verlag für Rechtsjournalismus GmbH*, Muster Datenschutzerklärung, https://www.datenschutz.org/datenschutzerklaerung-muster.pdf.

Teil. 3 - Handlungsempfehlungen

1 Empfehlungen / Auswirkungen

Aufgrund der umzusetzenden Maßnahmen sowie dem erheblichen Mehraufwand ist es erforderlich und auf jeden Fall ratsam, ein adäquates und regelmäßiges Audit durchzuführen, das in die künftige Planung eingeht. Nur dadurch ist gewährleistet, dass die adäquate Umsetzung der Datenschutz-Grundverordnung und der damit verbundene Mehraufwand regelmäßiger Überprüfung derselben Beachtung findet.

Aufgrund von Verfehlungen im Bereich der Datenschutz-Grundverordnung kam es in den Folgejahren der Einführung im Jahr 2018 (25.05.2018) seitens der nationalen Aufsichtsbehörden bereits zu mehreren erheblichen Bußgeldern. Mehr noch, durch diese und weitere Maßnahmen der Datenschutzbehörden ist mittlerweile klar geworden, dass die Datenschutz-Grundverordnung nun in allen Bereichen überprüft und zur Anwendung gelangt. Die Auswirkungen auf die Bereiche der Geschäftsleitung, IT / Technik sowie der Personalabteilung werden nachfolgend erläutert. Darüber hinaus erfolgt eine Handlungsempfehlung für den Datenschutzbeauftragten eines Unternehmens.

1.1 Geschäftsleitung

Welche und wie viele Ressourcen wofür verwendet werden ist Aufgabe der Geschäftsleitung eines Unternehmens und schlussendlich liegt dieses in der Verantwortung einer Konzernleitung, sofern diese Bestandteile der Unternehmensstruktur sind. Gleiches gilt für die Budgetverantwortung der verantwortlichen Personen. Diese muss schließlich durch die Geschäftsleitung vertreten, kommuniziert, erklärt und eingehalten werden. Nur sollte unter keinen Umständen versäumt werden, die Mitwirkung des Verantwortlichen für die Verarbeitung Verantwortlichen wie auch des Datenschutzbeauftragten zur Planung hinzu zu ziehen. Gemäß Art. 38 Abs. 3 Satz 1 DS-GVO ist der Datenschutzbeauftragte weisungsfrei, dieses bezieht sich explizit auf die Ausübung der Tätigkeit. Nach Art. 39 DS-GVO hat der Datenschutzbeauftragte die Aufgabe das Unternehmen und den oder die Verantwortlichen zu beraten. Um diese Beratungstätigkeit ausüben zu können, ist es

notwendig und ratsam, die erforderlichen Mittel bereit zu stellen. Nur durch eine konsequente Überprüfung und Umsetzung der Datenschutz-Grundverordnung können Fehler vermieden werden. Zur Erarbeitung der Lösung eines juristischen Sachverhalts dient das Gutachten. Das Gutachten soll sich unter Abwägung aller in Betracht kommender Aspekte Schritt für Schritt zu einer Entscheidung durcharbeiten. Dabei macht es keinen Unterschied, ob ein konkreter Fall oder ein allgemeines juristisches Problem zu lösen ist.[1196]

Welche Mittel erforderlich sind, um eine vernünftige Datenschutzpolitik durchführen zu können muss in einer angemessenen Art und Weise analysiert werden. Handelt es sich dabei um einmalige Aufwendungen oder sind diese als wiederkehrende Positionen in die künftige Planung aufzunehmen?

Folgende Positionen sind im Bereich der Datenschutz-Planung und Umsetzung bzw. Korrektur zu berücksichtigen:

1.1.1 Personalplanung

Möglicherweise wurde die Einstellung weiterer Mitarbeiterinnen und Mitarbeiter regelmäßig verschoben. Könnte durch die Einführung der Datenschutz-Grundverordnung dieser Umstand korrigiert werden? So insbesondere immer wiederkehrend im technischen Bereich. Bei aktuellen und künftigen Kalkulationen des zusätzlichen einzustellenden Personals sollten möglichst alle Variablen beachtet werden. Handelt es sich bspw. um eine Vollzeit- oder Teilzeitkraft, wie viel Urlaub wird angesetzt, wie hoch ist die durchschnittliche Krankheitsdauer? Gerne werden Annahmen getroffen, die von einer Produktivität von regelmäßigen 100 % ausgeht. Es muss eigentlich jedem Manager bewusst sein, dass Personen, die einer immer wiederkehrenden Tätigkeit nachgehen, nicht in der Lage sind, regelmäßig 100 % zu leisten. In der Folge könnte dieses bedeuten, dass die Produktivität von Mitarbeiterinnen und Mitarbeiter durch zusätzliches Personal variieren kann, sie muss es nicht zwangsläufig.

1196 *Gola/Reif,* Praxisfälle Datenschutzrecht, 2. Aufl. 2016, S. 21, Abschnitt II, Punkt 1 (Gutachten) Abs. 1.

1.1.2 Variante Datenschutzbeauftragter

Welche Variante des Datenschutzbeauftragten sollte gewählt werden und aus welchem Grund?

Hier muss zwischen der internen und der externen Variante unterschieden werden. Damit verbunden die Kosten für die externe Variante und den entsprechenden Anreisen, Schulungen und Informationsmaterial oder ist für die entsprechende Struktur die Wahl des internen Datenschutzbeauftragten die Bessere. Hierbei gilt abzuwägen, welche Entscheidung tatsächlich die bessere Wahl ist, allerdings immer bezogen auf die jeweilige Unternehmensstruktur. Der Datenschutzbeauftrage muss dieser Aufgabe aus freien Stücken nachkommen wollen. Mit dem Ausdruck, „Bestellung“ ist nicht gemeint, dass jede im Unternehmen tätige Person den Weisungen der Geschäftsleitung zur Übernahme der Aufgabe des Datenschutzbeauftragten nachkommen muss, weil diese es bestimmt.

1.1.3 Technisch Organisatorische Maßnahmen

Welche **t**echnisch **o**rganisatorischen **M**aßnahmen (**TOM**) müssen zwingend umgesetzt werden und welche sind einfach, „nice to have“?

Hier „lauert“ in der Regel die größte Unsicherheit, da es hier um Veränderungen der bestehenden technischen Landschaft geht. Sollte hier aus welchen Gründen auch immer im Vorfeld nicht exakt analysiert worden sein, was und wie umgestellt, angeschafft oder schlicht eingeschaltet werden muss, könnte dieses zu bösen Überraschungen führen.

In einer Zeit in welchen das Homeoffice als überwiegendes Büro genutzt wird ist zu prüfen, wie es sich aktuell und während dieser Phasen mit den Themen des Datenschutzes verhält. Hieran schließt die Frage, sind die für den beruflichen Teil sowie die privaten Einstellungen datenschutzkonform? Ist das eigene Kabel basierende private Netzwerk sowie das privat genutzte Wlan (Wireless local area network) gegen äußere Einflüsse gesichert? Wie verhält es sich mit personenbezogenen Daten bei möglichem Zugriff durch Familienmitglieder / Lebenspartner oder Abschnittsgefährten? Hat bspw. jedes Mitglied der Gemeinschaft einen eigenen Account oder benutzen alle Mitglieder denselben Zugang?

Die aktuelle Zeit zeigt sehr deutlich die technischen Möglichkeiten des Durchführbaren auf. Da Mitarbeiterinnen und Mitarbeiter, Geschäftspartner, Freunde und Bekannte sich nicht persönlich sehen dürfen, wird das Medium der **Videokonferenz** gerne genutzt. Hierzu ist insbesondere zu überprüfen, welche Software in welchem Netzwerk auf

welcher Basis benutzt wird. Konferenzen und oder Vorstellungsgespräche mit der Geschäftsleitung müssen wie bei einer „normalen Konferenz“ bzw. „Vorstellungsgespräch“ geplant und überprüft werden. Hierbei ist im Besonderen auf die verschlüsselte Übertragung besonders schutzwürdiger Daten zu achten. Nicht alle Programme zur Nutzung einer Videokonferenz sind automatisch datenschutzkonform erstellt.

Wie verhält es sich bei Vorstellungsgesprächen mit einem im **nicht europäischen Ausland** befindlichen Mitarbeiter oder Mitarbeiterin? Wurden hierzu alle Belange überprüft und als sicher eingestuft oder bestehen Zweifel bei der Kommunikation mit dem Land, welches die Infrastruktur des Videopartners stellt? Gewissheit über die Zulässigkeit und der Sicherheit entsprechend der Übertragung sowie der Einwilligung müssen im Vorfeld überprüft und als Datenschutzkonform bestätigt werden. Die Nutzer US-Amerikanischer Systeme sollten sich vergewissern, dass diese Systeme und Programme gemäß dem aktuellen EU – US. Privacy Shield (Nachfolgeabkommen des Safe Harbour Abkommens [1197]) zertifiziert sind. Andere Länder benötigen ein ähnliches Zertifikat. Gemäß der aktuellen Datenschutz-Grundverordnung ist es vorgeschrieben, dass ein Auftragsverarbeitungsvertrag abgeschlossen wird. Dieses entlässt niemanden aus der Verantwortung die genutzten Systeme auch kritisch zu hinterfragen.

Aus diesem Grund ist es entsprechend wichtig hierzu eine Vereinbarung abzufassen, um alle möglichen Unklarheiten auszuräumen. Nachfolgendes Muster einer Vereinbarung beinhaltet alle erdenklichen Punkte, die selbstverständlich auf das entsprechende Unternehmen angepasst werden muss.

1197 N. *Jung,* Abolition of the Safe Harbour Agreement: Legal situation and alternatives, http://hdl.handle.net/10419/148370.

1.1.4 Richtlinie Home-Office / Mobile-Office (Telearbeit)

§ 1 Gegenstand der Richtlinie, Allgemeines

(1) Diese Richtlinie regelt Fragen des Datenschutzes und der Datensicherheit, wenn Mitarbeitern ein Arbeitsplatz in der eigenen Wohnung oder ein mobiler Arbeitsplatz (Home - Office / Mobile - Office – folgend zusammenfassend „Heimarbeitsplatz“) durch [Arbeitgeber] zur Verfügung gestellt wird. Sie ergänzt die allgemeinen betrieblichen Bestimmungen zu Datenschutz und Datensicherheit, die auch am Heimarbeitsplatz stets einzuhalten sind. Im Fall von Widersprüchen geht diese Richtlinie vor.

(2) Ein Heimarbeitsplatz darf nur zur Verfügung gestellt und genutzt werden, wenn die dort zu leistende Tätigkeit zur Erledigung außerhalb des Betriebs geeignet ist, insbesondere mit Blick auf Datenschutz- und Datensicherheitsaspekte. In jedem Fall ist eine schriftliche Vereinbarung mit dem betroffenen Mitarbeiter erforderlich.

(3) Ein Heimarbeitsplatz darf nur zur Verfügung gestellt und genutzt werden, wenn der Mitarbeiter eine Schulung über Datenschutz und Datensicherheit bei Nutzung von Heimarbeitsplätzen absolviert hat, die in angemessenen Abständen zu wiederholen ist. Ist eine solche Schulung ausnahmsweise nicht erforderlich, darf ein Heimarbeitsplatz auch mit Zustimmung des betrieblichen Datenschutzbeauftragten zur Verfügung gestellt und genutzt werden.

§ 2 Umgang mit Daten

(1) Auch wenn Mitarbeiter an ihrem Heimarbeitsplatz tätig werden, bleiben sie Teil von [Arbeitgeber]. Dies bedeutet, dass alle vertraglichen Weisungsrechte bestehen bleiben und insbesondere alle betrieblichen Daten, Informationen und Unterlagen, im Hoheitsbereich von [Arbeitgeber] verbleiben. Allen Mitarbeitern ist es daher untersagt, betriebliche Daten, Informationen oder Unterlagen – insbesondere personenbezogene und sonst vertrauliche Daten – an Dritte weiterzugeben, sie Dritten zur Kenntnis gelangen zu lassen (etwa durch Einsichtnahme am Bildschirm oder auf Ausdrucken), sie auf eigenen Speichermedien abzuspeichern, unbefugt zu kopieren oder zu anderen als betrieblichen Zwecken zu verwenden.

(2) Insbesondere

- ist es verboten, Dritten Passwörter oder sonstige Zugangsmöglichkeiten zur dienstlichen EDV (z. B. Chipkarten) mitzuteilen oder zugänglich zu machen, z. B. durch Notieren von Passwörtern oder Lagerung der Chipkarte am Lesegerät;
- ist es verboten, Dritten (z. B. Familienmitgliedern, sonstigen Mitbewohnern, Besuchern) Zugriff auf die betriebliche EDV und/oder betriebliche Unterlagen zu gewähren;
- ist es untersagt, betriebliche Daten auf anderen Speichermedien als von [Arbeitgeber] schriftlich zugelassen zu speichern; zugelassen ist die Speicherung auf betrieblichen Servern (Laufwerk […]). Verboten ist somit insbesondere die Speicherung von betrieblichen Daten auf privaten Smartphones, USB-Sticks, Computern o. ä.;
- ist es verboten, dienstliche Daten mit privaten Geräten zu verarbeiten; dazu gehört auch der Abruf des dienstlichen E-Mail-Accounts mit einem privaten Computer, Smartphone o. ä.;
- ist es verboten, Sicherheitsmaßnahmen zu deaktivieren oder zu umgehen oder sonstige technische Veränderungen an den durch [Arbeitgeber] zur Verfügung gestellten Geräten vorzunehmen. Software darf nur durch die IT-Abteilung installiert werden;
- müssen eventuelle Ausdrucke mit vertraulichen Informationen (z. B. personenbezogenen Daten) sicher vernichtet werden, wenn sie nicht mehr benötigt werden (Aktenvernichter).

(3) Alle Störungen oder Auffälligkeiten bei der EDV-Nutzung sind unverzüglich der IT-Abteilung zu melden.

(4) Die private Nutzung der für den Heimarbeitsplatz bereitgestellten betrieblichen Geräte bzw. Zugangsmöglichkeiten (insbesondere Computer und Internetzugang) ist verboten.

(5) [Arbeitgeber] ist jederzeit berechtigt, vom Mitarbeiter die Herausgabe sämtlicher betrieblicher Daten, Unterlagen und Akten einschließlich sämtlicher Kopien zu verlangen; sind zum Zugriff auf betriebliche Daten Passwörter oder sonstige Schlüssel erforderlich, sind diese mit herauszugeben. Der Mitarbeiter kann hiergegen kein Zurückbehaltungsrecht geltend machen.

§ 3 Sicherheitsmaßnahmen im Home-Office

(1) Als Heimarbeitsplatz in der Wohnung des Mitarbeiters darf nur ein Raum genutzt werden, der abschließbar ist. Er soll bei Nichtnutzung durch den Mitarbeiter abgeschlossen werden. Hat der Mitarbeiter Gäste (auch Handwerker) in seiner Wohnung, muss der Raum verschlossen sein. Halten sich Dritte am Heimarbeitsplatz auf (z. B. Handwerker, die hier arbeiten müssen), muss der Mitarbeiter sie jederzeit beobachten.

(2) Verlässt der Mitarbeiter seinen Heimarbeitsplatz (und sei es nur kurz, etwa zur Toilette), muss sichergestellt sein, dass kein Dritter auf betriebliche Daten oder Akten zugreifen kann. Dies bedeutet insbesondere, dass

- der verwendete Computer gesperrt werden muss, so dass bei Rückkehr zumindest die Eingabe des Passwortes erforderlich ist;
- Fenster verschlossen sein müssen, außer bei kurzzeitiger Abwesenheit, während der ein Eindringen realistischerweise ausgeschlossen werden kann (z. B. 10. Stock und keine Möglichkeit, aus der Nachbarwohnung herüberzuklettern);
- bei Nutzung von Papier-Akten diese in einem Schrank einzuschließen sind oder der Heimarbeitsplatz-Raum abzuschließen ist; dies gilt nur dann nicht, wenn der Mitarbeiter allein zu Hause ist und seinen Heimarbeitsplatz nur kurzzeitig verlässt;
- bei Verlassen der Wohnung ein gegebenenfalls genutztes Zugangsmedium (z. B. Chipkarte, Transponder) vom Computer entfernt werden muss und bei Nutzung von Papier-Akten diese in einem Schrank einzuschließen sind.

§ 4 Zusätzliche Sicherheitsmaßnahmen im Mobile-Office

Bei der Nutzung eines mobilen Arbeitsplatzes (Mobile - Office) außerhalb der Wohnung des Mitarbeiters gilt ergänzend zu den Regelungen in § 3:

(1) Der Mitarbeiter darf den mobilen Arbeitsplatz außerhalb eines verschlossenen Raumes nicht – auch nicht kurzzeitig – unbeaufsichtigt lassen, wenn nicht eine Aufsicht durch einen anderen Mitarbeiter von [Arbeitgeber] sichergestellt ist. Ausnahmsweise kann der Vorgesetzte Ausnahmen zulassen, wenn der mobile Arbeitsplatz an feste oder ausreichend große Gegenstände angeschlossen, eine ausreichende soziale Kontrolle sichergestellt, die Abwesenheit nur kurz ist und keine besonders vertraulichen Daten verarbeitet werden.

(2) Bevor der Mitarbeiter seine direkte Aufmerksamkeit vom mobilen Arbeitsplatz entfernt, ist der Computer zu sperren und sind alle Zugangsmedien (z. B. Chipkarte, Transponder) zu entfernen und sicher zu verwahren.

(3) Die mobile Nutzung von Akten bedarf der vorherigen [schriftlichen] Zustimmung des Vorgesetzten. Diese darf nur erteilt werden, wenn der betriebliche Datenschutzbeauftragte im Einzelfall oder für eine bestimmte Art von Akten, gegebenenfalls beschränkt auf einen bestimmten Nutzungsort, zugestimmt hat.

(4) Die Mitnahme des mobilen Arbeitsplatzes ins Ausland bedarf der Zustimmung des Vorgesetzten und des betrieblichen Datenschutzbeauftragten, wenn nicht der betriebliche Datenschutzbeauftragte in Abstimmung mit der Geschäftsführung für sämtliche Ziel- und Transitländer eine allgemeine Freigabe erteilt hat.

§ 5 Sicherheitsmaßnahmen beim Transport und bei der Übertragung von Akten und *Daten*

(1) Jede Mitnahme betrieblicher Daten und Akten benötigt die vorherige [schriftliche] Zustimmung des Vorgesetzten.

(2) Nimmt der Mitarbeiter betriebliche Akten mit, dürfen diese nur in verschlossenen Behältnissen transportiert werden (z. B. verschlossene Kiste, verschlossener Aktenkoffer). Der Mitarbeiter darf die Akten beim Transport zu keiner Zeit unbeaufsichtigt lassen. Dies gilt auch, wenn das verschlossene Behältnis im Kofferraum eines Autos transportiert wird (z. B. ist ein Verlassen des Fahrzeugs zum Einkaufen auf dem Heimweg nicht zulässig).

(3) Nimmt der Mitarbeiter betriebliche Daten mit, muss der Datenträger mit einem von der IT-Abteilung freigegebenen Verfahren nach dem Stand der Technik verschlüsselt sein.

(4) Jede Datenübertragung zwischen dem Heimarbeitsplatz und dem Betrieb – einschließlich Terminal-Zugriff – muss nach dem Stand der Technik verschlüsselt sein. Hierfür trägt die IT-Abteilung Sorge.

(5) Zugriffe und Zugriffsversuche vom Heimarbeitsplatz werden von [Arbeitgeber] protokolliert und regelmäßig ausgewertet. Diese Daten werden nur zur Missbrauchsentdeckung, -bekämpfung und -verfolgung verwendet und nicht zur Leistungs- oder Verhaltenskontrolle.

§ 6 Kontroll- und Zutrittsrechte zur Wohnung

(1) Der Mitarbeiter räumt folgenden Personen das Recht ein, zur Kontrolle des Heimarbeitsplatzes seine Wohnung zu betreten:

a. zur Kontrolle der Arbeitssicherheit einer von [Arbeitgeber] hierfür gesondert beauftragten Person;
b. zur Kontrolle der Datensicherheit dem betrieblichen Datenschutzbeauftragten;
c. zur Einrichtung, Wartung, Reparatur, Änderung, Abholung der von [Arbeitgeber] bereitgestellten Arbeitsmittel der IT-Abteilung bzw. sonstigen hierfür gesondert beauftragten Personen;
d. zu den gesetzlich vorgesehenen Kontrollen allen Behörden, die den Heimarbeitsplatz aufsuchen dürften, wenn sich dieser im Betrieb befände, beispielsweise der Datenschutz-Aufsichtsbehörde;
e. dem Betriebsrat, wenn er eine der unter a) bis d) genannten Personen begleitet.
f. Das Zutrittsrecht ist auf den Heimarbeitsplatz (einschließlich zugehöriger Einrichtungen, etwa Telefonanschluss im Keller o. ä.) begrenzt und auf das unbedingt Erforderliche zu beschränken. Jeder Zutritt ist rechtzeitig im Voraus abzustimmen, wobei auf die Interessen des Mitarbeiters, wie beispielsweise Kinderbetreuung, Rücksicht zu nehmen ist, und auf Werktage zwischen 8:00 Uhr und 18:00 Uhr zu beschränken, es sei denn, aus besonderen Gründen ist ein sofortiger oder kurzfristiger Zutritt oder ein Zutritt zu einem bestimmten Termin unbedingt erforderlich. Im Fall des Zutrittsrechts nach S. 1 lit. d) (Behörden) richten sich eventuelle Abstimmungspflichten und Zeiten nach den Befugnissen der Behörde, die diese hätte, wenn sich der Heimarbeitsplatz im Betrieb befinden würde, und beschränken sich die Pflichten von [Arbeitgeber] darauf, den Mitarbeiter unverzüglich zu informieren, sobald ihm der Zutrittswunsch bekannt wird, und auf Wunsch des Mitarbeiters zur Behörde zu vermitteln, um einen anderen Termin zu vereinbaren.

(2) Die Erlaubnis zur Einrichtung und Nutzung des Heimarbeitsplatzes steht zudem unter der aufschiebenden Bedingung, dass (der Heimarbeitsplatz kann also erst eingerichtet werden, wenn) sämtliche Mitbewohner des Mitarbeiters die gleichen Zutrittsrechte einräumen. [Arbeitgeber] kann jederzeit verlangen, dass der Mitarbeiter die Zustimmung aller Mitbewohner schriftlich nachweist.

(3) Widerruft der Mitarbeiter oder einer seiner Mitbewohner das Zutrittsrecht oder kommt ein neuer Mitbewohner hinzu, der nicht die Zutrittsrechte nach Abs. 1 einräumt, erlischt automatisch die Berechtigung des Mitarbeiters, den Heimarbeitsplatz zu nutzen. Der Mitarbeiter ist verpflichtet, dies sofort [Arbeitgeber] anzuzeigen, sämtliche betrieblichen Akten und Datenträger sofort in den Betrieb zurückzubringen und seine Arbeitsleistung auf Wunsch von [Arbeitgeber] im Betrieb zu erbringen.

(4) Widerruft der Mitarbeiter oder einer seiner Mitbewohner das Zutrittsrecht oder kommt ein neuer Mitbewohner hinzu, der nicht die gleichen Zutrittsrechte einräumt, kann [Arbeitgeber] zudem verlangen, dass der Mitarbeiter unverzüglich sämtliche von [Arbeitgeber] bereitgestellten Arbeitsmittel auf eigene Kosten in den Betrieb zurückbringt.

§ 7 Beendigung der Heimarbeitsplatz-Nutzung

(1) Enden die Berechtigung des Mitarbeiters zur Nutzung des Heimarbeitsplatzes oder das Arbeitsverhältnis oder wird der Mitarbeiter unwiderruflich von der Pflicht zur Arbeitsleistung freigestellt, hat der Mitarbeiter unaufgefordert unverzüglich sämtliche betrieblichen Zugangsmedien (z. B. Chipkarten, Transponder), Datenträger und Akten (einschließlich Kopien) in den Betrieb zurückzubringen und dem Vorgesetzten zu übergeben. Sind zum Zugriff auf betriebliche Daten Passwörter oder sonstige Schlüssel erforderlich, sind diese mit zu übergeben.

(2) Der Mitarbeiter hat zudem die Abholung sämtlicher von [Arbeitgeber] bereitgestellter Arbeitsmittel durch von [Arbeitgeber] beauftragte Personen nach angemessener Ankündigungsfrist zu dulden.

§ 8 Hinweis auf rechtliche Folgen bei Verstößen

[Arbeitgeber] weist darauf hin, dass Verstöße gegen diese Richtlinie nicht nur arbeitsrechtliche Folgen (Ermahnung, Abmahnung, fristgerechte oder fristlose Kündigung) haben, sondern auch mit Geldbuße bedroht und/oder strafbar sein können (z. B. im Fall des Kopierens von Daten nach Art. 83 DS-GVO, § 42 BDSG, § 17 UWG [gegebenenfalls: § 203 StGB]). Darüber hinaus können Verstöße gegen diese Richtlinie Unterlassungs- und Schadensersatzansprüche nach sich ziehen.[1198]

1.1.5 Schulungen

Weiterhin stellt sich die Frage der durchzuführenden Schulungen. Fallen einmalige **Schulungen** sowie den damit verbundenen Kosten an oder müssen diese als regelmäßige Position in die Planung aufgenommen werden?

Es ist anzunehmen, dass einige Unternehmen hierzu nur das dringend erforderliche geplant haben, um erst einmal den Anforderungen der Umsetzung der Datenschutz-Grundverordnung Genüge zu tun. Eine langfristige Personalplanung bzw. Personalentwicklungsplanung sollte auf jeden Fall das Mittel der Wahl sein. Zu hinterfragen ist:

- Wer führt die Schulungen durch?
- Müssen alle Mitarbeiterinnen und Mitarbeiter zur selben Zeit an der Maßnahme teilnehmen oder ist dieses in der vorherrschenden Struktur überhaupt nicht möglich?
- Müssen Schulungen sowie Auffrischungsseminare in jedem Jahr besucht werden oder ist eine auf zwei oder drei Jahre ausgelegte Variante nicht auch ausreichend?
- Finden die Schulungen im eigenen Büro / Unternehmen statt oder müssen hier Reisekosten und oder Übernachtungskosten mit eingeplant werden?
- Kann durch technische Gegebenheiten und entsprechender Infrastruktur eine Schulung nicht auch in Teilen Online absolviert werden. Dadurch würde sich die Belastung aller beteiligten Personen um ein Vielfaches reduzieren. (Dieses nur, wenn die Entsendung der Personen nicht auch als „Dankeschön“ für geleistete Arbeit bzw. Verdienste für das Unternehmen genutzt werden soll)

1198 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, Bergt, S. 352 ff.

Einige Anbieter organisieren Seminare und Schulungen in anspruchsvolleren Hotels um die Maßnahme sowie den Aufenthalt **angenehm** gestalten zu können. Diese Kosten sind entweder in die Seminar- / Schulungsgebühren integriert oder müssen separat entrichtet werden. In der Konsequenz bedeutet dieses lediglich, dass die Leitung des Unternehmens, bereits im Vorfeld über den Umfang informiert sein muss, um eine entsprechende Bewertung der Situation vornehmen zu können. Ein Verstoß gegen die Schulungspflicht des Arbeitgebers **kann** mit einem **Bußgeld** von bis zu **10 Millionen** geahndet werden.

Dabei ist es durchaus gängige Praxis in einigen Bereichen Schätzungen abzugeben, sollten die tatsächlichen Aufwendungen und Erträge vorab nicht kalkulierbar sein. Eine Schätzung wird, bei nicht vorhanden Referenzdaten, in Bereichen durchgeführt, die von **nicht beeinflussbaren Faktoren** bestimmt sind, bspw. Flughäfen, Parkhäuser, Hotels oder ähnliche Bereiche, um nur einige zu nennen. So zu beobachten während der aktuellen Corona-Pandemie (Covid. 19, 2020).

1.1.6 Überprüfung der Unternehmensstrukturen

Sollten die aktuellen **Unternehmensstrukturen**, die möglicherweise bereits mehrere Jahre vorhanden und in Teilen sehr erprobt sind, in diesem Zusammenhang nicht auf eine **flexiblere Form** umgestellt werden oder genügen diese den Anforderungen des Datenschutzes?

Wie im Abschnitt, **Changemanagement** aufgezeigt wurde, ist es ebenfalls sinnvoll, die **eigenen Strukturen** durchaus einmal **in Frage** zu **stellen**. Es ist ebenfalls die Aufgabe der Unternehmensleitung, das Unternehmen „**zukunftssicher**“ zu gestalten. Natürlich ist es schwierig, die kommenden Jahre richtig zu beurteilen, insbesondere bei **nicht beeinflussbaren Faktoren**. Allerdings müssen auch hier so viele Informationen, Zahlen und Fakten zusammengetragen werden, wie erforderlich sind, um eine adäquate Prognose abgeben zu können. Denn nichts anderes wird von der Unternehmensleitung in diesem Bereich tatsächlich erwartet.

Kann der **Datenschutzbeauftragte**, sofern die **fachliche und persönliche Eignung** vorliegt, auch für **andere Gesellschaften im Konzernverbund** tätig werden, um dadurch den Kostenblock des Datenschutzes verringern zu können?

Dieses gestaltet sich immer dann etwas schwierig, wenn sich die weiteren Unternehmenseinheiten nicht national, sondern international aufgestellt sind. Bei nationaler Aufstellung sind Sitten, Gebräuche sowie Arbeitsweisen und lokale Gesetze

bekannt. Es kommen in der Regel keine Überraschungen auf den Datenschutzbeauftragten zu. Ein im europäischen Ausland ansässiges Unternehmen mit einem national agierenden Datenschutzberater betreuen zu wollen, könnte sich als kontraproduktiv herausstellen. Dieses ist im Besonderen für Länder, die außerhalb der Europäischen Union aufgestellt sind, zu beachten.

1.1.7 Synergien

„Arbeitet" jede Einheit (Abteilung) autark oder können auch hier **Synergien** verwendet werden? Weiterhin muss über mögliche Verstöße als kalkulierbares Risiko nachgedacht werden. Können bspw. die **72 Stunden** die zur Meldung von Verletzungen nach **Art. 33 DS-GVO** vorgeschrieben sind, **jederzeit** eingehalten werden?

Menschen gehen in Urlaub, Menschen werden krank oder machen einfach Fehler. Wie verhält es sich in Krisensituationen? Welche Person ist persönlich bzw. fachlich geeignet oder springt einfach ein und macht sich evtl. schadenersatzpflichtig? Mangelnde oder fehlerhafte Technik bzw. fehlende Kenntnisse in den entsprechenden Bereichen / Abteilungen sind nicht das Problem der Datenschutzbehörden. Ein Unternehmen und deren Vertreter müssen jederzeit sicherstellen, dass in Abwesenheit des Verantwortlichen, der Datenschutz nicht einfach brach liegt. Der bloße Hinweis auf eine „dünne Personaldecke" kann nicht bedeuten, dass alles auf dem Rücken der Kunden, Mitarbeiterinnen und Mitarbeiter ausgetragen werden kann. Bei externen Modellen des Datenschutzbeauftragten ist dies das Problem des beauftragten Unternehmens. Dieser muss aus Gründen der Haftung auf eine interne Redundanz aufbauen. Bei internen Modellen muss der Arbeitgeber Sorge dafür tragen, dass bei Urlaub, Krankheit oder schlicht Weggangs des Datenschutzbeauftragten sichergestellt ist, dass die Überwachung und Beratung uneingeschränkt und ohne Zeitverlust weitergeht.

1.1.8 Datenschutzerklärung

Wurde eine entsprechende **Datenschutzerklärung** erstellt?

Eine den Anforderungen der Datenschutz-Grundverordnung angemessene Datenschutzerklärung kann nicht durch einen Mitarbeiter oder Mitarbeiterin ohne Kenntnisse der Materie erstellt werden. Das reine Kopieren einer „fremden" Datenschutzerklärung mit Änderungen in unternehmensspezifischen Bereichen, ist ebenfalls wenig ratsam. Eine Datenschutzerklärung muss der aktuellen Rechtslage entsprechend unter Berücksichtigung der aktuellen Anforderungen erstellt werden. Die Anforderungen an

die Datenschutzerklärung richten sich immer nach den unternehmensspezifischen Besonderheiten. Auch hier gilt es zu beachten, dass eine Nicht-Erstellung oder eine vorsätzlich fehlerhaft erstellte Datenschutzerklärung ein Bußgeld in Höhe von bis zu 20 Millionen Euro nach sich ziehen kann. Eine Mustervorlage einer Datenschutzerklärung befindet sich im Anhang dieser Arbeit. Die ist lediglich als Muster anzusehen und muss entsprechend angepasst und vor Nutzung durch entsprechende Fachleute überprüft werden.

1.1.9 Risikoabwägung

Das Risiko auf Grundlage der Datenschutz-Grundverordnung mit einem Bußgeld belangt zu werden, hängt in der Regel von unterschiedlichsten Faktoren ab. Nachfolgend einige Punkte die bei der Risikoabwägung beachtet werden müssen:

- Wie ist die Schwere der Datenschutzverletzung einzuschätzen und wie lange hielt diese an?
- Wie viele Personen betrifft die Datenschutzverletzung?
- Welcher Schaden entstand durch die Verletzung der Datenschutz-Grundverordnung?
- Hat das Unternehmen vorsätzlich gehandelt im Wissen um die Verfehlung?
- Wurde seitens des Unternehmens versucht den Schaden zu begrenzen oder wurden die Konsequenzen billigend in Kauf genommen?
- Liegen mehrere Verstöße vor oder handelt es sich um einen einzigen Verstoß?
- Handelt es sich um eine einmalige Verfehlung?
- Hat die Zusammenarbeit mit dem Datenschutzbeauftragten des Unternehmens auf kooperativer Basis stattgefunden?
- Wurde der Verstoß selbständig innerhalb der geforderten Frist gemeldet (72 Stunden) ?
- Sind mildernde Umstände gegeben?[1199]

Die nationalen Aufsichtsbehörden haben begonnen, die Unternehmen aufgrund der Informationen, die zur jeweiligen Anzeige geführt haben, abzuarbeiten. In der

1199 *Die eRecht24 GmbH wird vertreten durch: Rechtsanwalt Sören Siebert, Dipl.-Wirtsch.-Inf. Karsten Fernkorn.*

Konsequenz sollten im Jahr 2020 alle Auflagen der Datenschutz-Grundverordnung vollumfänglich umgesetzt sein. Die oben aufgeführten Beispiele sind nur auszugweise dargelegt. Es existieren erheblich mehr Verstöße mit den damit verbundenen Bußgeldern, als allgemein angenommen wird. Natürlich werden einige Unternehmen, aus verständlichen Gründen, Einspruch gegen die entsprechenden Bußgeldbescheide einlegen. In der Konsequenz wird abzuwarten sein, wie die entsprechenden Gerichte zu den jeweiligen Entscheidungen urteilen werden.

1.2 IT / Technik

In Erwägungsgrund 83 der Datenschutz-Grundverordnung in Zusammenhang mit Art. 24 und Art. 32 der DS-GVO sowie § 64 BDSG sind die Auflagen für die Sicherheit der personenbezogenen Daten aufgeführt und geregelt. Die technisch organisatorischen Maßnahmen können aufgrund der Komplexität nicht in einigen wenigen Sätzen wiedergegeben werden. Es ist essenziell, dass die entsprechenden Absätze in Teil II, **TOM** (**t**echnisch **o**rganisatorische **M**aßnahmen) oder durch andere externe Quellen, vorab technisch erfasst werden können. Ansonsten würde es schwierig werden, die Materie umfänglich erfassen zu können.

Erwägungsgrund 83 besagt:

Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine diese Verordnung verstoßende Verarbeitung sollte der Verantwortliche oder der Auftrags-Verarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen. Diese Maßnahmen sollten unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau, auch hinsichtlich der Vertraulichkeit gewährleisten, dass den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Bei der Bewertung der Datensicherheitsrisiken sollten die mit der Verarbeitung personenbezogener Daten verbundenen Risiken berücksichtigt werden, wie etwa ob unbeabsichtigt oder unrechtmäßig Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung oder von unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte.

In der Konsequenz wird ein erheblicher Aufwand erforderlich, um die gesamte Bandbreite der genannten Bereiche vollumfänglich erfassen zu können. Sinnvoll ist in diesem Zusammenhang, ein „ehrliches Audit“ und eine kritische Hinterfragung der tatsächlichen Vorgänge. Auch wenn diese Maßnahmen bei Einführung der Datenschutz-Grundverordnung am 25.5.2018 erfolgt sind, hat dieses nicht zur Folge, dass der „Status quo“ nicht weiter geprüft und auf den aktuellen Stand der Technik gebracht werden muss.

Durch Veränderung der technischen Systeme, auch wenn es sich nur um Upgrades im Software Bereich handelt, können durchaus datenschutzproblematische Lücken aufgewiesen werden. Die geänderten aktuellen Arbeitsbedingungen waren mit an

Sicherheit grenzender Wahrscheinlichkeit niemals Grundlage einer all umfassenden Überprüfung. Auch wenn die aktuelle Situation, Ausnahmetatbestände ermöglichen und eine wahrscheinlich nicht stattfindende Überprüfung bedeutet, kann dieses nicht die Grundlage der eingeführten Maßnahmen bilden. Durch Homeoffice, Videokonferenzen, Einsatz der eigenen Software und Hardware (Bring Your Own Device), private Netzwerke sowie Schwierigkeiten bei der Bestimmung der Nutzer der geschaffenen Infrastruktur, ist es wahrscheinlich, dass in der langen Kette der potenziell neuralgischen Punkte, einige Bereiche ungeprüft genutzt werden. Mit Rückkehr zur „Normalität“ im Jahr 2020 müssen diese Systeme und Infrastrukturen unbedingt einer umfassenden Prüfung unterzogen werden. Ansonsten besteht die Möglichkeit einer Überprüfung durch die Aufsichtsbehörden zum Zwecke der Feststellung der umgesetzten Maßnahmen.

Sollten einzelne Bereiche nicht den Vorgaben der Datenschutz-Grundverordnung entsprechen, so muss unverzüglich und vollumfassend Bericht erstattet und die Aufsichtsbehörden informiert werden. Ein Audit in den entsprechenden Bereichen kann die Schwachstellen offenbaren, sofern diese tatsächlich auch gesehen werden wollen. Es ist unumgänglich, die erste Analyse unter Zuhilfenahme einer Checkliste zu erstellen. Nur dadurch kann erst ermessen werden, wie weit der zu prüfende Bereich reicht.

1.2.1 Technisch Organisatorische Maßnahmen

Die rechtlichen Anforderungen der Datenschutz-Grundverordnung sind ausführlich in den Teilen I und II dargelegt. Im dritten Teil sollen einige allgemeine Handlungsempfehlungen aufgeführt und erläutert werden, die im allgemeinen Sprachgebrauch gängiger Natur sind.

1. Wurde eine **Dokumentation** zu allen umgesetzten und eingeführten Maßnahmen erstellt und wird diese regelmäßig (in der Regel einmal im Quartal) überprüft und aktualisiert?
2. Wurde ein **Löschkonzept** erstellt und findet dieses Anwendung? (siehe Bußgeld Deutsche Wohnen SE)
3. Wurden alle neuralgischen Zugänge hinsichtlich einer **Zutrittskontrolle** überprüft? Hier gilt im Besonderen zu bedenken, dass bei fragmentierten Unternehmen, die beispielsweise mehrere Parkhäuser und Tiefgaragen in unterschiedlichen Städten betreiben, eine lokale Geldverarbeitung stattfinden kann. Dabei handelt es sich bei Filialen und oder selbstständigen Einheiten auch um die Technikräume in welchen Alarmanlagen sowie Videoüberwachung

zusammenkommen. Gleiches gilt für die Schlüsselverwaltung bzw. Schließsysteme. Diese müssen in einem speziellen Sicherheitsschrank abgelegt werden. Der Zugangsschlüssel oder Code sollte allerdings nicht in den angrenzenden Schubladen der Schreibtische abgelegt werden. Denn das würde ein eventuelles Sicherheitskonzept ad absurdum führen.

4. Auf welcher Grundlage hat die Umsetzung der **Datenweitergabe** erfolgt? Hierbei geht es im Besonderen aber nicht ausschließlich um E-Mail Versand, deren Verschlüsselung sowie möglichen **VPN**-Netzwerken (**V**irtual **P**rivat **N**etwork). VPN Netzwerke sind in der Regel als sehr sicher einzustufen. Die Verbindung von bspw. zwei Anwendern wird nach Verbindungsaufbau über ein VPN Netzwerk verschlüsselt. Es ist **in der Regel** nicht möglich von außen auf diese Verbindung zugreifen zu können. Einziges Problem ist, dass die Log-Dateien der VPN-Systeme die persönlichen Daten der Nutzer speichern. Diese Log-Dateien müssen ebenfalls unter Zuhilfenahme von Passwörtern und Zugriffskontrollen gesichert werden. Problematisch wird dieses bei Netzwerkanbietern außerhalb der Europäischen Union. Beispielsweise sind die Betreiber eines VPN-Netzwerkes verpflichtet alle Log-Daten, die über deren Server laufen, zu speichern. In diesen Fällen sollte überprüft werden, inwieweit die Datenschutz-Grundverordnung eingreifen kann. Hier ist der Art. 3 DS-GVO bezüglich der räumlichen Anwendung zu überprüfen.
5. Bezüglich der sogenannten **Eingabekontrolle** ist die Definition des BDSG zu Hilfe zu nehmen: „*Die Speicherkontrolle soll die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Verändern und Löschung von gespeicherten Datenverhindern. Die Eingabekontrolle soll gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogene Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert wurden*“.[1200] Dabei handelt es sich um die Erfassung aller „berechtigten Personen“ welchen eine Nutzung aller Systeme zur Erfassung personenbezogener Daten eingeräumt wurde. Werden Daten eingegeben, verändert oder gar gelöscht, muss das bestehende System

1200 *Eßer/Kramer/Lewinski* (Hrsg.), DSGVO/BDSG, Kramer/Meints, S. 1846, Rn. 17 (Speicherkontrolle und Eingabekontrolle, § 64 Abs. 3 Satz 1 Nr. 3 und 7 BDSG).

dieses aufzeichnen und protokollieren (Log-Dateien). Bei der Auswertung ist aus Sicherheitsgründen darauf zu achten, dass regelmäßig mindestens zwei Personen anwesend sind. Diese Aufgabe muss in der Regel durch den Datenschutzbeauftragten durchgeführt werden oder in Kombination mit einem Verantwortlichen.

6. Bei der **Trennungskontrolle** handelt es sich um ein Gebot Daten die getrennt verarbeitet wurden auch in unterschiedlichen Datenbanken und am besten auch auf unterschiedlichen Datenträgern zu sichern. Der für die Verarbeitung Verantwortliche muss sicherstellen, dass die zu unterschiedlichen Themen erhobenen Daten auch getrennt verarbeitet werden.[1201] Dieses gilt auch für die Nutzung mobiler Geräte die sinnvollerweise nicht für den privaten und dienstlichen Bereich gleicherweise genutzt werden.
7. Dem Thema, **Auftragsverarbeitung**, kommt besondere Bedeutung zu, da diese nicht ausschließlich die Organisation und Einhaltung der Datenschutz-Grundverordnung des eigenen Unternehmens betrifft. Es besteht eine Verpflichtung, die technisch organisatorischen Maßnahmen des Auftrags-Verarbeiters zu prüfen. Hier muss vor Abschluss eines Vertrages eine „Vorab-kontrolle“ vorgenommen werden, um zu prüfen, ob alle Datenschutzrelevanten Punkte erfüllt sind. Nur nach eigehender Überprüfung können Verträge über eine entsprechende Zusammenarbeit abgeschlossen werden.
8. Ein wichtiges Konzept der technisch organisatorischen Maßnahmen bezieht sich auf die Möglichkeit der **Datenwiederherstellung**. Dabei geht es im Grunde um die Backup Struktur des Unternehmens und wie diese aufgebaut und verwaltet wird. In Abhängigkeit der entsprechenden Unternehmensstruktur werden unterschiedlichste Modelle umgesetzt. Waren in der Vergangenheit „lediglich“ Backup Systeme auf Basis eines Serversystems aufgestellt, findet heute eine Erweiterung der Infrastruktur statt. Die Möglichkeit einer Datenspeicherung über Cloud Anbieter und oder lokale Serverfarmen reduziert die Möglichkeiten eines Datenverlustes erheblich. Aber auch hier gilt zu beachten, dass Serverfarmen und Cloudsysteme auf Datensicherheit überprüft werden müssen. Dabei gilt es erneut

1201 *Reimann/e.V.,* Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung, 2. Aufl. 2018, S. 78 Abschnitt 5.2.7 Trennungskontrolle.

die Besonderheiten des jeweiligen Landes zu beachten. Anbieter derartiger Systeme müssen, um mit einem in der Europäischen Union ansässigen Unternehmen, die Datenschutzkonformität beachten. Die Risiken eines Datenverlustes sollten auf jeden Fall im Risikomanagement betrachtet und bewertet werden. Der Verlust von wirtschaftlich relevanten Daten und / oder personenbezogenen Daten der Kunden, kann durchaus zu einer Schieflage des betroffenen Unternehmens führen. Verbunden mit den Auflagen der Datenschutz-Grundverordnung können hier erhebliche Bußgelder verhängt werden.

9. Sind die **IT-Verantwortlichen** entsprechend der aktuellen Anforderungen ausgebildet oder wurden diese entsprechend geschult. Wurde im Risikomanagement die Vertretung adäquat gelöst? Die Position des Verantwortlichen für die IT ist eine der Schlüsselpositionen in einem Unternehmen. Hier laufen fast alle Fäden, die für eine erfolgreiche Umsetzung der technisch organisatorischen Maßnahmen erforderlich sind, zusammen. Sind diese Position und der entsprechende Vertreter fachlich und persönlich nicht geeignet, kann dieses zu erheblichen Problemen und in der Folge zu Schwierigkeiten mit den Aufsichtsbehörden führen.
10. Besteht eine ausreichend hohe **Systemsicherheit** bezogen auf die IT-Systeme? Alle Systeme müssen in regelmäßigen Abständen einem „Stresstest“ unterzogen werden. Nur dadurch wird eine Sicherheitslücke und in der Folge eine Abstellmaßnahme entwickelt. Die Wiederholung derartiger Tests sollten in Abhängigkeit einer Gefährdungsanalyse durchgeführt werden. Aus diesem Grund kann eine entsprechende Empfehlung über die Frequenz derartiger Prüfungen nicht abgegeben werden.
11. Werden regelmäßige Audits über die technisch organisatorischen Maßnahmen durchgeführt? Wie bereits mehrfach erläutert sollten Veränderungen in der Struktur der IT regelmäßig überprüft und auf Datenkonformität hin überprüft werden. Die Sicherheit kann nur durch regelmäßige strukturierte Überprüfungen vorgenommen werden. Aus der Erfahrung sind derartige Prüfungen durch ein Audit verbunden mit einer erfolgreichen Zertifizierung gegeben.

1.2.2 Privacy by Design

Die rechtliche Bewertung sowie die Anforderungen finden sich in einigen Kapiteln dieser Arbeit. Hintergrund für diese Anforderung, liegt bereits in der Planung der gesamten Struktur bezogen auf die Datenschutz-Grundverordnung. Dieses bedeutet, dass bereits in der Entwicklungsphase für die geplanten Anschaffungen von Software, Hardware oder ähnlichem, darüber nachgedacht werden muss, wie diese Anforderungen der Datenschutz-Grundverordnung beeinflussen werden. Hier werden in der Regel Punkte wie bspw. **Datenminimierung** angeführt. Diese Steuerungsinstrumente knüpfen direkt an die Technikgestaltung an. Die Verpflichtung umfasst sowohl physische wie auch Online-Dienste. So wird Herstellern von datenverarbeitenden Produkten auferlegt, bereits bei der Planung sowie Umsetzung die Datenschutzauflagen zu beachten.[1202]

1.2.3 Privacy by Default

Darunter ist die Verpflichtung des Verantwortlichen zu verstehen, **konfigurierbare** Arbeitsweisen seiner Produkte so zu gestalten, dass in der **Voreinstellung** nur personenbezogene Daten verarbeitet werden, die auch tatsächlich für den konkreten Verarbeitungszweck erforderlich sind. Möchte der Nutzer (betroffene Person) weitere Produkte nutzen, so müssen diese durch den Nutzer aktiv ändern oder einstellen. Als Beispiele kann der Kauf eines Betriebssystems oder Mobiltelefon angeführt werden. Die eingestellte Grundeinstellung **muss aktiv geändert werden**, wenn der **Auslieferungszustand** geändert werden soll. So im Besonderen bei der regelmäßigen Übertragung der Standortdaten eines Mobiltelefons an den Hersteller oder bei zusätzlich genutzten Programmen. Die Standard Einstellung muss in diesem Fall beim „Einrichten" des Geräts aktiv geändert werden. Dabei werden zusätzliche Einwilligungen erforderlich die aus rechtlichen Gründen dokumentiert werden. Dieses aktive Eingreifen in die Default-Einstellung wird als sogenanntes **„Opt-In"** bezeichnet[1203]. Bereits voreingestellte Bestätigungskästchen sind hier nicht ausreichend. Derartige Fälle müssen grundsätzlich als Ablehnung der Installation bzw. der Einstellungsänderung konfiguriert sein. Die betroffene Person muss dieses aktiv auf „ich nehme an" oder „ich willige ein" umstellen oder anklicken. Eine Voreinstellung, die durch schnelles Klicken und oder

1202 *Schläger/Thode* (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 293, Rn. 758 (Art. 25 DSGVO).

1203 *Schläger/Thode* (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, S. 156, Rn. 364.

Bestätigen nicht bereits Datenschutzkonform ausgelegt ist, kann ein Bußgeld nach sich ziehen.

1.2.4 Cookies

Hinsichtlich eines Einsatzes von Cookies auf der entsprechenden Website ist dringend angeraten, die aktuelle Gesetzeslage zu überprüfen. Mit dem aktuellen Urteil des **Eu**ropäischen **G**erichts**h**ofes, C-673/17 (**EuGH**) sowie der in diesem Jahr erwarteten ePrivacy-Verordnung 2020, ist der Umgang mit Cookies im Besonderen zu prüfen und zu analysieren.

Vorab sollte überprüft werden, ob ein Einsatz von Cookies auf der eigenen Webseite überhaupt erforderlich ist. Mit einem Einsatz von Cookies ist zu klären, welcher Art die Cookies sein sollen bzw. müssen. Obwohl die Erforderlichkeit von Cookies nicht abschließend geklärt wurde, ist die Nutzung bzw. der Einsatz von nachfolgenden Cookies (dringend erforderliche Cookies) aktuell noch zulässig.

- Warenkorb-Cookies (bspw. die eines Online-Shops)
- Login-Daten und Status einer Community
- Sprachauswahl einer internationalen Webseite (im Wissen darum, dass dieser Cookie möglicherweise mehr übertragen kann als lediglich die Auswahl)
- Daten (Cookies) über die Einwilligung des Nutzers von Cookies

Der EuGH erläutert in seinem Urteil, dass die bloße Zustimmung und oder einem Abwählen von speziellen Cookies nicht ausreichend sei. Es ist erforderlich, dass der Internetnutzer zu den erforderlichen Cookies aufgeklärt werden muss und nicht durch simples An- und Abwählen eines Kästchen sein Einverständnis erteilt (vgl. Opt-Out und Opt-In Verfahren). Der Vorgang des Einverständnisses ist für jede Maßnahme separat vorzunehmen.

Ob dieser Umstand praktikabel ist, lässt sich zum aktuellen Zeitpunkt nicht vollständig darlegen. Die aktuelle Meinung, insbesondere die der Webseitenbetreiber, sehen hier einen dringenden Korrekturbedarf.

Bezüglich der Einwilligung sind nachfolgende Punkte im Besonderen zu beachten:

- Art und Funktionsweise
- Ablaufdatum und damit zeitliche Begrenzung
- Identität der Dienstleister (hier sind auch alle weiteren Dienstleister anzugeben, die die Cookies für ihre eigenen Zwecke verwenden (erste, zweite, dritte … -Partei)

Wer sich einmal die Mühe macht und den Einsatz von Cookies auf der besuchten Webseite zu überprüfen, wird feststellen, dass hier in einigen Fällen sehr viele Cookies eingesetzt werden. Viele dieser Cookies sind bereits per Haken in den entsprechenden Kästchen voreingestellt. Zum aktuellen Zeitpunkt ist die Einwilligung über das sogenannte Opt-In (eigenes Tätigwerden durch das Anklicken eines Kästchens) bzw. Opt-Out (Verwendung von bereits angeklickten Kästchen) -Verfahren im Cookie-Banner, alternativ über eine Registrierung, geregelt. Nun führt der EuGH aus, dass nicht nur personenbezogene Daten sondern auch Tracking-Daten einer Einwilligung bedürfen. Dabei sollte nicht die Informationspflicht gemäß Art. 13 und 14 DS-GVO vergessen werden. In der Folge ist anzumerken, dass der Umgang mit Cookies nicht einfacher geworden ist. Die ePrivacy-Verordnung 2020, welche eigentlich mit Einführung der Datenschutz-Grundverordnung, aktualisiert werden sollte, wird aller Voraussicht nach erst im Jahr 2020 veröffentlicht werden. Dabei handelt es sich wie bei der Datenschutz-Grundverordnung um eine Verordnung und nicht wie bei den Vorgängerversionen um Richtlinien. Eine Übergangfrist wie bei der Datenschutz-Grundverordnung wird es nicht geben. Somit wirkt diese unmittelbar und in Verbindung mit der Datenschutz-Grundverordnung sowie nationalen Regelungen.

Das Cookie-Pop-Up Fenster muss künftig adäquat platziert werden. Das Fenster darf unter keinen Umständen das Impressum oder die Datenschutzerklärung verdecken und nur durch das Bestätigen der Cookies die Ansicht freigeben. Die Webseiten-Besucher sollen ohne eine Einverständniserklärung abgegeben zu müssen, Zugriff auf die erforderlichen Informationen haben können.

Der Umgang mit Cookies ist in allen Internet-Browsern einstellbar und einsehbar. Es steht dem Nutzer frei (allerdings verbunden mit dem Verlust des gewohnten Komforts bei Aufrufen der Seiten), einzelne Cookies zu löschen oder in ihrer Wirkung einzuschränken.

1.3 Personalabteilung

Der Aufgabenkatalog einer Personalabteilung ist sehr vielfältig. Hier geht es meist nicht nur um die reinen personalbezogenen Aufgaben, sondern in vielen Fällen auch um Planung, Entwicklung und Betreuung. Die Anwendungen und Entwicklungen eines Entgeltsystems sind ebenfalls in der Personalabteilung angesiedelt. Somit handelt es sich um diejenige Abteilung, welche den intensivsten Kontakt mit personenbezogenen Daten hat.

Die Kernprozesse in der Personalarbeit sind die Grundlagen, um einen geeigneten Mitarbeiter für ein Unternehmen zu gewinnen, ihn zu halten und zu entwickeln, bis er das Unternehmen wieder verlässt.[1204] Diese Vorgehensweise ist entsprechend wichtig, da gute oder exzellente Mitarbeiter aufgrund der genannten Maßnahmen das Unternehmen auswählen, um dort tätig zu werden. Darüber hinaus sind derartige Personalentwicklungsmaßnahmen in der Außendarstellung die ideale Werbung, um neue Talente gewinnen zu können. Der Verzicht auf eine adäquate Personalentwicklung, bspw. aus Kostengründen, führt in den meisten Fällen nicht zur Idealbesetzung einer Position. Einem hoch qualifizierten Anwärter sollten alle erdenklichen Entwicklungsmöglichkeiten aufgezeigt werden, so dass dieser auf Grundlage der gewonnen Informationen eine entsprechende Entscheidung treffen kann.

1.3.1 Betriebsvereinbarungen

Betriebsvereinbarungen werden durch den Art. 88 DS-GVO sowie dem BetrVG und ausdrücklich auch durch den § 26 BDSG geregelt. In Abs. 2 der DS-GVO wird folgendes ausgeführt: „umfassen geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz.“

1204 *Höf-Bausenwein,* Crashkurs Personalarbeit - inkl. Arbeitshilfen online, 3. Aufl. 2018, S. 12, Abs. 1 Satz 1.

Das Wirtschaftslexikon Gabler definiert den Begriff der **Betriebsvereinbarung** wie folgt:

„Die Betriebsvereinbarung ist das vorrangige Instrument zur Ausübung der betrieblichen Mitbestimmung …“ [1205]

Die Betriebsvereinbarung wird in der Regel zwischen dem Arbeitgeber und der Arbeitnehmervertretung (Betriebsrat) geschlossen. Existiert allerdings ein Tarifvertrag für die entsprechende Branche ist dieser vorrangig zu beachten. In der Datenschutz-Grundverordnung wird die Betriebsvereinbarung ebenfalls als „**kollektive Regelung**“ bezeichnet. Dadurch besteht die Möglichkeit, auf freiwilliger Basis den **Erlaubnisrahmen** zu schaffen, um Beschäftigtendaten verarbeiten zu können. In Unternehmen, in welchen keine Arbeitnehmervertretung existent ist, bedeutet dieses meist, dass zwischen Arbeitgeber und den einzelnen Beschäftigten **individuelle** Vereinbarungen geschlossen werden können.

Der Erwägungsgrund 155, der ergänzend zu Artikel 88 DS-GVO die erforderlichen Auflagen ausführt, wird inhaltlich wie folgt dargelegt. „Im Recht der Mitgliedstaaten oder in Kollektivvereinbarungen (einschließlich ’Betriebsvereinbarungen) **können spezifische Vorschriften** für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorgesehen werden, und zwar insbesondere Vorschriften über die Bedingungen, unter denen **personenbezogene Daten** im **Beschäftigungskontext** auf der **Grundlage der Einwilligung des Beschäftigten** verarbeitet werden dürfen, über die Verarbeitung dieser Daten für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses.“[1206]

1205 *Springer Gabler Verlag* (Hrsg.), Betriebsvereinbarung, Was ist Betriebsvereinbarung?, Gabler Wirtschaftslexikon, https://wirtschaftslexikon.gabler.de/definition/betriebsvereinbarung-28363/version-251995.

1206 Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgrund 155 DSGVO.

Das **Betr**iebs**v**erfassungs**g**esetz besagt, dass die Einwilligung in einem Beschäftigungsverhältnis nicht greifen kann, wo die Zulässigkeitsgrenzen durch Betriebs- oder Dienstvereinbarung, ohne das Persönlichkeitsrecht des Arbeitnehmers in unzulässiger Weise einzuschränken (§ 75 Abs. 2 **BetrVG**), im kollektiven Interesse einheitlich festgelegt worden sind.[1207]

Das Unternehmen, **H&M** (**H**ennes und **M**auritz) steht aktuell im Fokus der Hamburger Datenschutzbehörde.[1208] Das Unternehmen soll seine MitarbeiterInnen systematisch ausgespäht haben. Dabei wurden private Daten über Krankheit sowie familiäre Daten erhoben. Die Hamburger Datenschutzbehörde hat aus diesem Grund ein Bußgeldverfahren eingeleitet, dessen Ausgang aktuell nicht geklärt ist. Betroffen sei ein Nürnberger Call – Center. Es kann hier aufgrund eines erheblichen Verstoßes zu einem entsprechenden Bußgeld führen, welches auf Grundlage des Vorjahresumsatzes berechnet werden würde.

Die Personalverwaltung in Zusammenarbeit mit dem Verantwortlichen und oder dem Datenschutzbeauftragten haben hier eine Informations- und Beratungsverantwortung gegenüber der Geschäftsleitung. Die Notwendigkeit einer Betriebsvereinbarung mit ihren notwendigen Auflagen, Urteilen und Gesetzen müssen im Detail beachtet werden. Ein Bußgeld aufgrund einer nicht zulässigen Verarbeitung der Beschäftigtendaten kann ein erhebliches Bußgeld mit sich ziehen. (siehe Bußgeldverfahren H&M)

Eine Muster-Vorlage zur Betriebsvereinbarung „**Videoüberwachung**“ kann im **Anhang** eingesehen werden. Diese kann nach Anpassung - und auf Grundlage der Datenschutzgesetze - als Vorlage bzw. Vereinbarung genutzt werden. Bei einem derart komplexen Thema ist eine Überprüfung durch fach- und sachkundige Spezialisten (bspw. Rechtsanwälte) unumgänglich.

1.3.2 Personalakten

Wie im Kapitel, Beschäftigtendatenschutz, unter dem Abschnitt, Personalakte, dargelegt wurde, besteht seitens des Arbeitgebers keine Verpflichtung zur Führung umfangreicher

---

1207 *Gola,* Handbuch Beschäftigtendatenschutz, 8. Aufl. 2019, S. 151, Rn. 509, Abschnitt 4 Entgegenstehende Betriebsvereinbarung.

1208 Bußgeldverfahren gegen H&M (Hennes & Mauritz), Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Pressemitteilung vom 26.01.2020, https://datenschutz-hamburg.de/medienbildung_news/h_m/.

Sammlungen von auf das Arbeitsverhältnis bezogene Daten und Vorgängen.[1209] Die Pflicht zur Führung von Personalakten ist für den öffentlichen Dienst für Beamte gesetzlich vorgesehen, wobei auch der Begriff der Personalakte definiert wird.[1210]

Bereits im Bundesbeamtengesetz unter § 106 ist die Personalakte definiert. Darin enthalten sind die wesentlichen Punkte, die zur Führung der Personalakte erforderlich sind. Absatz 1 des § 106 BBG führt hierzu aus:

„… Sie ist vertraulich zu behandeln und durch **t**echnische und **o**rganisatorische **M**aßnahmen (**TOM**) nach den Artikeln 24, 25 und 32 der Verordnung (EU) 2016 / 679[1211] des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung vor unbefugter Einsichtnahme zu schützen.“[1212]

Das Betriebsverfassungsgesetz und seine für die Privatwirtschaft betreffende Norm, wird im § 83 BetrVG geregelt. § 83 BetrVG beinhaltet lediglich zwei wichtige Rechtspositionen der Beschäftigten. Diese sind ein Informationsrecht bezüglich Inhalt der Akte und zum anderen ein Gegendarstellungsrecht gegenüber dem Inhalt der Akte.[1213] Diese sind allerdings immer wieder Grundlage für diverse Streitigkeiten und enden meist durch die Beurteilung durch die entsprechenden Gerichte.

Satz 1 Absatz 1 des § 83 führt aus: *„Der Arbeitnehmer hat das Recht, in die über ihn geführten Personalakten Einsicht zu nehmen*.“ Ergänzend hierzu aus Absatz 2*: „Erklärungen des Arbeitnehmers zum Inhalt der Personalakte sind dieser auf sein Verlangen beizufügen.*[1214] Weiterhin ist anzuführen, dass die in § 83 BetrVG geregelten

1209 *Gola,* Handbuch Beschäftigtendatenschutz, 8. Aufl. 2019, S. 44, Rn. 7.
1210 *Gola,* Handbuch Beschäftigtendatenschutz, 8. Aufl. 2019, S. 513, Rn. 2359, Kapitel 15.
1211 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).
1212 Bundesbeamtengesetz, vgl. § 106 BBG Abs. 1.
1213 Betriebsverfassungsgesetz vom 2020, vgl. § 83 BetrVG.
1214 Betriebsverfassungsgesetz vom 2020, vgl. § 83 BetrVG.

Transparenz- und Korrekturregelungen bezüglich des Akteninhalts, dahingehend nicht verpflichtend sind, dass solche Akten auch geführt werden müssen.

Auf Grundlage von Transparenz und Datenminimierung sollte die Personalabteilung aufgebaut sein. Wobei das Thema der Datenminimierung immer auch eine Sache der Interpretation ist. Werden Personen zur Notwendigkeit einer Personalakte befragt und auf deren Inhalt angesprochen, werden die Wenigsten die Überflüssigkeit der Inhalte anführen. Aus diesem und weiteren Gründen sind hierzu der Gesetzgeber sowie die bereits geurteilten Verfahren zu beachten.

Nicht alle Datenerhebungen sind zulässig.[1215] Es empfiehlt sich, die Personalakte nach sachlichen Gesichtspunkten in Grundakte und Teilakte zu gliedern. Die Grundakte sollte nur solche Schriftstücke und Daten der Beschäftigten enthalten, die für den Werdegang bedeutsam sind, wie Personalbogen und Unterlagen über Ausbildung, bisherige Tätigkeit oder Dienstzeitberechnung. Sie sollte bei der personalbearbeitenden Dienststelle geführt werden. Teilakten können für bestimmte Sachgebiete angelegt werden, etwa für Besoldung/Gehalt, Reisekosten oder Beihilfe, und sollten bei den für die Bearbeitung sachlich zuständigen Stellen geführt werden. Die Seiten der Personalgrundakte sind zu nummerieren, damit die Vollständigkeit nachweisbar ist.[1216]

1215 *Der Landesbeauftragte für Datenschutz und Informationsfreiheit, Mecklenburg-Vorpommern,* Personalakten und Personalaktendaten, https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/persakte.pdf.

1216 Gesetz zur Regelung des Statusrechts der Beamtinnen und Beamten in den Ländern, vgl. § 50 Personalakte - BeamtStG.

In einer Personalakte dürfen nachfolgende Unterlagen enthalten sein. Da die Grundlage auf dem Bundesbeamtengesetz beruht, sind Begrifflichkeiten aus diesem Bereich aufgeführt.

- Personalbogen
- Bewerbungsschreiben, Lebenslauf, Lichtbild
- Personenstandsurkunden und ggf. Nachweis über die Staatsangehörigkeit
- Nachweise über Schulbildung sowie Aus- und Fortbildung einschließlich der Prüfungszeugnisse
- Gesundheitszeugnisse und ärztliche Stellungnahmen zur gesundheitlichen Eignung für einen Dienstposten, Nachweis der Schwerbehinderteneigenschaft, Unterlagen über Dienstunfälle
- Unterlagen über Erkrankungen
- Unterlagen über Vereidigung, Ernennung, Abordnung, Zuweisung, Versetzung, Umsetzung, Übertragung eines Dienstpostens, Teilzeitbeschäftigung, Ermäßigung der Arbeitszeit, Urlaub, Dienstjubiläum, Nebentätigkeiten, ehrenamtliche Tätigkeiten, Ehrungen, Belobigungen
- dienstliche Beurteilungen, Zeugnisse - Vorgänge über mit dem Beschäftigungsverhältnis zusammenhängende Beschwerden, Behauptungen und Bewertungen, die zutreffend und relevant sind
- abschließende Entscheidungen in Rechtsstreitigkeiten aus dem Beschäftigungsverhältnis
- Unterlagen über Straf-, Berufsgericht- oder Bußgeldverfahren, soweit ein Bezug zur dienstlichen Tätigkeit besteht
- abschließende Entscheidungen in Regressverfahren
- abgeschlossene Disziplinarvorgänge
- Besoldungs-/Gehaltsvorgänge einschließlich der Vorgänge über Abtretungen, Pfändungen, Verpfändungen, Gehaltsvorschüsse
- Unterlagen über Trennungsgeld, Umzugskostenvergütung, Reisekostenvergütung
- Unterlagen über Unterstützungen und Zuschüsse

- Unterlagen über die Entlassung oder die Versetzung in den Ruhestand
- Vorgänge über die Versorgung Hinterbliebener
- Abrechnungen der freien Heilfürsorge
- Anträge und Beschwerden in persönlichen Angelegenheiten.[1217]

Personalakten dürfen aufgrund ihres sensiblen Inhaltes nur sicher aufbewahrt werden. Sie sind vertraulich zu behandeln und müssen gegen unbefugte Einsichtnahme geschützt werden. Eine weiterführende Nutzung der Personalakte, bspw. eine digitale Übermittlung an die Konzernmutter kann nur durch Einwilligung des Betroffenen erfolgen.

Folgende Urteile des Bundesarbeitsgerichts ermöglichen einen Überblick über die Komplexität einer Personalakte.

BAG – URTEIL, 9 AZR 271/06 VOM 12.09.2006

1. Der Arbeitnehmer hat gemäß §§ 12, 862, 1004 BGB Anspruch auf Beseitigung der ungeschützten Aufbewahrung seiner Gesundheitsdaten in der Personalakte. Denn hierdurch wird in sein durch Art. 1 und 2 GG gewährleistetes allgemeines Persönlichkeitsrecht eingegriffen. Der Arbeitgeber ist deshalb verpflichtet, sensible Daten über den Arbeitnehmer in besonderer Weise aufzubewahren. Sie sind gegen zufällige Kenntnisnahme, etwa durch Aufbewahrung in einem verschlossenen Umschlag, zu schützen. Der informationsberechtigte Personenkreis ist zu beschränken.

2. Dem steht nicht das berechtigte Interesse des Arbeitgebers an der Vollständigkeit der Personalakte entgegen. Denn die Personalakte bleibt vollständig. Bei berechtigtem Anlass kann der Umschlag geöffnet und die Daten eingesehen werden.[1218]

1217 *Der Landesbeauftragte für Datenschutz und Informationsfreiheit, Mecklenburg-Vorpommern,* Personalakten und Personalaktendaten, https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/persakte.pdf.

1218 BGH - Bundesarbeitsgericht, 12 September 2006 – 9 AZR 271 / 06.

BAG – Urteil, 2 AZR 782/11 vom 19.07.2012

Der Arbeitnehmer kann die Entfernung einer zu Recht erteilten Abmahnung aus seiner Personalakte nur dann verlangen, wenn das gerügte Verhalten für das Arbeitsverhältnis in **jeder Hinsicht bedeutungslos** geworden ist.[1219]

1.3.3 Bewerbungen

Bewerber gelten datenschutzrechtlich als Beschäftigte. Ihre Unterlagen sind bis zur Entscheidung über die Einstellung bzw. bis keine Notwendigkeit mehr besteht diese aufzubewahren, relevant. Dabei ist zu klären, wie mit den personenbezogenen Daten umgegangen wird oder welche Daten überhaupt verwendet werden können. Dabei ist es unerheblich, welche Form der Datenerhebung verwendet wird. Viele Unternehmen sind dazu umgestiegen, digitale Bewerbungen zu präferieren. In der Konsequenz bedeutet dies, dass die eigenen Daten wie bspw. Lebenslauf und weitere personenbezogene Daten in einem umfangreichen Bewerbungsbogen abgefragt und erfasst werden. Eine generelle Datenerhebung ist nicht zulässig. Diese zu Unrecht erhobenen Daten sind in jedem Fall zu löschen. Die Speicherung bzw. Aufbewahrung sind an keine zeitliche Vorgabe geknüpft. Die erhobenen und für die Bewerbung relevanten Daten sind bis zur Beendigung des Auswahlverfahrens speicherbar. Aus Gründen möglicher Ansprüche abgelehnter BewerberInnen aus einem Bewerbungsverfahren sind Unterlagen weitere zwei Monate nach Beendigung aufzubewahren. Dieses ist in der Regel eine angemessene Frist. Darüber hinaus ist eine Speicherung nicht zulässig. Es ist in jedem Fall darauf zu achten, dass personenbezogene Daten unter keinen Umständen an oder von ehemaligen Arbeitgebern befreundete Unternehmen übermittelt bzw. angefordert werden oder gar archiviert oder zum Zwecke einer statistischen Erhebung erhoben werden ohne das die betroffene Person dieser Maßnahme **ausdrücklich** seine Zustimmung erteilt hat. Ohne eine Einwilligung mit Begründung einer Datenübermittlung an weitere Unternehmen ist dieses unzulässig. Hier greift der Grundsatz des „Verbots mit Erlaubnisvorbehalt“. Die Zulässigkeit der Fragen und derer die nicht zugelassen sind, werden in Teil II dieser Arbeit ausführlich dargestellt.

1219 Bundesarbeitsgericht - BAG, 19.07.2012 – BAG - 2 AZR 782/11.

Es wird ausdrücklich darauf hingewiesen, dass vor Beginn eines Bewerbungsverfahrens darauf hingewiesen wird, wie mit den erhobenen personenbezogenen Daten umgegangen wird und was mit diesen passiert, sollte die Bewerbung keinen Erfolg haben. Die hierfür erforderliche Einwilligung, nicht notwendiger Weise in Schriftform, aus Nachweisgründen allerdings angeraten, sollte in jedem Fall eingeholt und dokumentiert werden. Um mögliche datenschutzrelevante Notizen zu vermeiden kann in diesen Fällen anhand einer Liste gearbeitet werden. Hier können bspw. lediglich Nummern aufgrund einer Bewerberliste genutzt werden. Diese anonymisierte Liste kann unter strengen Auflagen erstellt und nur Anhand einer zugehörigen Verknüpfung entschlüsselt werden. Aus diesen und weiteren Gründen sehen einige Länder bereits von der Notwendigkeit eines Namens sowie eines Bewerbungsfotos ab. Dadurch werden zusätzlich zur datenschutzrechtlichen Bewertung auch Benachteiligung auf Grundlage von Rasse, Geschlecht oder Religion vermindert. Die Einwilligung kann durch eine Erklärung über die Verwendung der personenbezogenen Daten erfolgen. Gleiches gilt durch einen Datenschutzhinweis für die Bewerber sowie dem Bewerberverfahren.

Nachfolgendes **Muster** kann inhaltlich unter Berücksichtigung des Datenschutzrechts genutzt werden. Es empfiehlt sich, die Erklärung vor Nutzung auf rechtlicher Basis überprüfen zu lassen.

Einwilligungserklärung zur Speicherung von Bewerberdaten

Sollte meine Bewerbung nicht erfolgreich sein, willige ich ein, dass [Arbeitgeber] meine personenbezogenen Daten, die ich im Rahmen des gesamten Bewerbungsverfahrens mitgeteilt habe (zum Beispiel in Anschreiben, Lebenslauf, Zeugnissen, Bewerber-Fragebögen, Bewerber-Interviews), über das Ende des konkreten Bewerbungsverfahrens hinaus speichert. Ich willige ein, dass [Arbeitgeber] diese Daten nutzt, um mich später zu kontaktieren und das Bewerbungsverfahren fortzusetzen, falls ich für eine andere Stelle in Betracht kommen sollte.

Optional: Sofern ich in meinem Bewerbungsschreiben oder anderen von mir im Bewerbungsverfahren eingereichten Unterlagen selbst „besondere Kategorien personenbezogener Daten“ nach Art. 9 der Datenschutz-Grundverordnung mitgeteilt habe (z.B. ein Foto, das die ethnische Herkunft erkennen lässt, Angaben über Schwerbehinderten Eigenschaft, usw.), bezieht sich meine Einwilligung auch auf diese Daten. [Arbeitgeber] möchte allerdings alle Bewerber nur nach ihrer Qualifikation bewerten und bittet daher, auf solche Angaben in der Bewerbung möglichst zu verzichten.]

Optional:

Diese Einwilligung gilt zudem für Daten über meine Qualifikationen und Tätigkeiten aus allgemein zugänglichen Datenquellen (insbesondere berufliche soziale Netzwerke), die [Arbeitgeber] im Rahmen des Bewerbungsverfahrens zulässig erhoben hat.] Meine Daten werden nicht an Dritte weitergegeben.

Diese Einwilligung ist freiwillig und hat keine Auswirkungen auf meine Chancen im jetzigen Bewerbungsverfahren. Ich kann sie ohne Angabe von Gründen verweigern, ohne dass ich deswegen Nachteile zu befürchten hätte. Ich kann meine Einwilligung zudem jederzeit [– zum Beispiel online über das Bewerbungssystem –] widerrufen; in diesem Fall werden meine Daten nach Abschluss des Bewerbungsverfahrens unverzüglich gelöscht.

Zusatzerklärung bei besonderen Kategorien von Daten:

Meine Bewerbung bei [Arbeitgeber] enthält besondere Kategorien personenbezogener Daten (z. B. Angaben zum Familienstand, die Informationen über mein Sexualleben oder meine sexuelle Orientierung geben können; Angaben zu meiner Gesundheit; ein Foto, das Rückschlüsse auf meine ethnische Herkunft und ggf. meine Sehkraft und/oder Religion erlaubt; ähnlich sensible Daten im Sinne von Artikel 9 der Datenschutz-Grundverordnung). Meine Bewerbung darf daher in der vorliegenden Form nur mit meiner Einwilligung verarbeitet werden. Ich willige ein, dass [Arbeitgeber] die besonderen Kategorien personenbezogener Daten, die in meinem Bewerbungsschreiben und den beigefügten Unterlagen enthalten sind, zum Zweck der Durchführung des Bewerbungs-verfahrens verarbeitet. Diese Einwilligung dient ausschließlich dazu, die Bewerbung in ihrer vorliegenden Form überhaupt berücksichtigen zu können. Die Informationen werden keine Berücksichtigung im Bewerbungsprozess finden, soweit nicht – insbesondere bei Schwerbehinderten – eine gesetzliche Verpflichtung hierfür besteht.

Meine Daten werden nicht an Dritte weitergegeben. Ich bin nicht verpflichtet, diese Einwilligung zu erteilen und kann stattdessen eine um die besonderen Kategorien personenbezogener Daten bereinigte Bewerbung einreichen, ohne dass dies Auswirkungen auf meine Chancen im Bewerbungsverfahren haben. Ich kann meine Einwilligung ohne Angabe von Gründen verweigern und eine erteilte Einwilligung jederzeit widerrufen. Im Fall des Widerrufs werden meine von der Einwilligung umfassten Daten unverzüglich gelöscht. Im Fall der Nichterteilung oder des Widerrufs der Einwilligung kann meine bereits eingereichte Bewerbung allerdings nicht in der vorliegenden Form berücksichtigt werden.

Abbildung 24: Einwilligungserklärung zur Speicherung von Bewerberdaten [1220]

1220 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, Bergt, S. 810, Abschnitt H. Beschäftigtendatenschutz.

Das im Anhang befindliche Muster einer Datenschutzinformation für Bewerber zeigt die Besonderheiten auf, die notwendig sind das gesamte Spektrum der Datenschutz-Grundverordnung erfassen zu können. Auch hier noch einmal den Rat, diese durch eine juristisch ausgebildete Person erstellen zu lassen.

1.4 Datenschutzbeauftragte(r) / Verantwortliche(r)

1.4.1 Anforderungen an die Bestellung

Die Anforderungen an den Datenschutzbeauftragten sind gekoppelt an die persönlichen und fachlichen Eigenschaften. Eine Person, die als Datenschutzbeauftragter tätig sein möchte, sollte zusätzlich zu seinen fachlichen Qualifikationen in der Lage sein, komplexe juristische Sachverhalte transparent und leicht verständlich erklären zu können. Darüber hinaus ist es wichtig, dass der angehende Datenschutzbeauftragte das Thema kennt. Hier liegt die Krux bei der Beauftragung eines internen Datenschutzbeauftragten aus Gründen der Bequemlichkeit oder aus Kostengründen dieses nicht extern vergeben wird. Wie soll ein Mitarbeiter oder eine Mitarbeiterin ein derart komplexes Thema erfassen können, es sei denn es ist Bestandteil einer adäquaten Ausbildung. Des Weiteren ergeben sich möglicherweise bei der Bestellung einer „Leitenden Person" ebenfalls Probleme, da diese evtl. zur Erledigung eine nicht fachlich qualifizierte Person zur Unterstützung verpflichtet.

Arbeitgeber sollten auf eine geordnete und systematische Sammlung personenbezogener Daten ihrer Bewerber und Beschäftigten achten. Durch datenschutzkonforme Protokollierungs- und Löschkonzepte müssen personenbezogene Daten bei Auskunftsansprüchen und Berichtigungs- und Löschungsbegehren nicht mühselig zusammengesucht werden, sondern können in Kürze extrahiert und den Betroffenen zugänglich gemacht werden.[1221]

1.4.2 Bestellung eines Datenschutzbeauftragten

Die Datenschutz-Grundverordnung (DS-GVO) sieht eine Bestellpflicht nur für solche privaten Stellen vor, deren Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche eine regelmäßige und systematische Beobachtung von betroffenen Personen in großem Umfang erforderlich machen oder die Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 Abs. 1 DS-GVO in großem

1221 *Landesbeauftragter Für Datenschutz und Informationsfreiheit, Baden-Württemberg,* Beschäftigtendatenschutz: Zwischen wirtschaftlicher und persönlicher Abhängigkeit und informationeller Selbstbestimmung, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/Ratgeber-ANDS-2.-Auflage.pdf.

Umfang oder von Daten zu strafrechtlichen Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO zum Gegenstand haben.[1222]

Eine Bestellung hat auf Grundlage der folgenden Punkte zu erfolgen:

1. Die Verarbeitung der personenbezogenen Daten wird von einer Behörde bzw. öffentlichen Stelle durchgeführt,
2. Die Kernaufgaben des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters besteht in der Durchführung von Verarbeitungsvorgängen, welche aufgrund ihrer Art, ihres Umfangs und / oder ihrer Zwecke eine umfangreiche, regelmäßige und systematische Beobachtung von Betroffenen erforderlich machen,
3. die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters besteht in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von Daten über strafrechtliche Verurteilungen und Straftaten.[1223]

Nachfolgend befindet sich ein Muster[1224] für die Bestellung eines Datenschutzbeauftragten. Dabei handelt es lediglich um einen Vorschlag, der an die Gegebenheiten angepasst werden muss. Darüber hinaus ist eine rechtliche Überprüfung angeraten.

1222 *Gola,* Handbuch Beschäftigtendatenschutz, 8. Aufl. 2019, S. 106, Rn. 303.
1223 *RA Jaspers, Andreas /RAin Reif, Yvette, LL.M.* RDV / Recht der Datenverarbeitung Heft 2/April 2016, 61.
1224 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, Kremer/Sander, S. 71.

Bestellung als Datenschutzbeauftragter

§ 1

Die [Name des Verantwortlichen, Straße/Hausnummer, PLZ/Ort]

– im Folgenden Auftraggeber genannt –

bestellt hiermit [Name des zu benennenden Datenschutzbeauftragten]

– im Folgenden Beauftragter genannt –

ab dem Beginn des [ENTWEDER:] mit dem Beauftragten abgeschlossenen Arbeitsvertrags [ODER:] mit dem Beauftragten abgeschlossenen Dienstvertrags [ODER:] mit [Name des Dienstleistungsunternehmens, Straße/Hausnummer, Postleitzahl/Ort] abgeschlossenen Beratungsvertrags [ENDE DER VARIANTEN], also ab dem [Datum] [EVENTUELL ZUSÄTZLICH:] und bis zum [Datum] [ENDE DES ZUSATZES] zum Datenschutzbeauftragten gem. Art. 37 DS-GVO [EVENTUELL ZUSÄTZLICH:] und § 38 Abs. 1 BDSG n. F. Der Beauftragte wird seine Leistungen zur Wahrnehmung des Amtes als Datenschutzbeauftragter auf der Grundlage des vorgenannten Vertrags und der gesetzlichen Bestimmungen erbringen.

§ 2

Der Beauftragte wird für den Auftraggeber die in Art. 39 DS-GVO definierten Aufgaben eines Datenschutzbeauftragten erfüllen, darunter

- Unterrichtung und Beratung des [ENTWEDER:] Verantwortlichen [ODER:] Auftragsverarbeiters [ENDE DER VARIANTEN] und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DS-GVO sowie nach sonstigen anwendbaren Datenschutzvorschriften,
- die Überwachung der Einhaltung der DS-GVO, anderer anwendbarer Datenschutzvorschriften sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen,
- auf Anfrage Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und ihrer Durchführung gem. Art. 35 DS-GVO,
- Zusammenarbeit mit der Aufsichtsbehörde sowie

- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation bei der Datenschutz-Folgenabschätzung gem. Art. 36 DS-GVO und ggf. Beratung zu allen sonstigen Fragen.

[EVENTUELL ZUSÄTZLICH:] Der Beauftragte wird für den Auftraggeber zusätzlich die folgenden Aufgaben erfüllen:

- [weitere Aufgaben aufzählen].

§ 3

Der Beauftragte berichtet gem. Art. 38 Abs. 3 S. 2 DS-GVO unmittelbar der höchsten Managementebene des Auftraggebers. [BEI EINEM EXTERNEN BEAUFTRAGTEN ZUSÄTZLICH:] Der Beauftragte wird jedoch nicht weitergehend in den Betrieb des Auftraggebers eingebunden, insbesondere wird ihm kein Weisungsrecht gegenüber Beschäftigten des Auftraggebers eingeräumt. [ENDE DES ZUSATZES] Dem Beauftragten steht kein Recht zu, den Auftraggeber zu vertreten. Dem Auftraggeber ist bekannt, dass der Beauftragte in Ausübung seines Amtes keinem Weisungsrecht unterliegt, dass sich der Beauftragte durch ihm zu diesem Zweck ggf. vom Auftraggeber bereitgestelltes Hilfspersonal unterstützen lassen kann, dass er dem Beauftragten und seinem Hilfspersonal unverzüglich alle zur Erfüllung seiner Aufgaben und zur Erhaltung seines Fachwissens erforderlichen Ressourcen sowie den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen zur Verfügung zu stellen hat. Der Auftraggeber wird sicherstellen, dass der Beauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird. Dem Auftraggeber ist bekannt, dass er den Beauftragten gem. §§ 6, Abs. 4, 38 Abs. 2 BDSG n. F. nur bei Vorliegen eines wichtigen Grundes entsprechend § 626 BGB abberufen kann, wenn eine Benennungspflicht besteht.

§ 4

(1) Die vorliegende Benennung steht unter der auflösenden Bedingung, dass der in § 1 genannte, der Benennung zugrundeliegende Vertrag endet, [ENTWEDER:] durch eine Kündigung oder sonstige Erklärung des Beauftragten [ODER:] durch eine Kündigung oder sonstige Erklärung des [Name des Dienstleistungsunternehmens].

(2) [IM FALLE DES VERTRAGS MIT EINEM UNTERNEHMEN ZUSÄTZLICH:] Dem Beauftragten wird mitgeteilt, dass [Name des Dienstleistungsunternehmens] dem Auftraggeber vertraglich garantiert hat, dass dem Beauftragten in Ausübung seiner Tätigkeit als Datenschutzbeauftragter für den Auftraggeber keine Weisungen erteilt werden. Die vorliegende Benennung steht unter der weiteren auflösenden Bedingung, dass das Arbeits- bzw. Dienstverhältnis zwischen dem Beauftragten und [Name des Dienstleistungsunternehmens] endet, ungeachtet des Rechtsgrunds der Beendigung.

Für den Auftraggeber:

(Ort, Datum) (Unterschrift, Funktion des Unterzeichners)

Ich habe vorstehende Benennung zur Kenntnis genommen:

(Ort, Datum) (Unterschrift des Beauftragten)

1.4.3 Formvorschriften

Die Datenschutz-Grundverordnung sieht keine Formvorschriften bezüglich der Beauftragung eines Datenschutzbeauftragten vor. Das Bundesdatenschutzgesetz hingegen verlangt die Wahrung der Schriftform nach § 126 BGB. Der Gesetzgeber sieht im Bundesdatenschutzgesetz a.F. keine explizite Schriftform vor. Aus Gründen der Rechtssicherheit und der Dokumentation erscheint eine schriftliche Beauftragung mehr als sinnvoll.[1225]

Hierzu muss das Datum eingesetzt werden und von beiden Parteien unterzeichnet werden. Das Unternehmen wird von einem Vertretungsberechtigten vertreten. Aufgrund der besonderen Stellung des Datenschutzbeauftragten, wird kein Enddatum in der Beauftragung angeführt. Die Datenschutz-Grundverordnung sieht keine Vorgaben für eine Abberufung des Datenschutzbeauftragten vor. Möglich ist eine definierte Übergangzeit in besonderen Fällen. Darüber hinaus ist die Vertretungsregelung schriftlich festzulegen.

1.4.4 Dauer der Bestellung

Die Position des Datenschutzbeauftragten wurde in einem ersten Entwurf aus dem Jahr 2012 für eine Mindestdauer von zwei Jahre festgelegt. Während seiner Amtszeit sollte er seines Postens nur dann enthoben werden können, wenn er die Voraussetzungen für die Erfüllung seiner Pflichten nicht erfüllt. Die Anforderungen bezüglich einer Mindestdauer der Bestellung sind im Rahmen der Trilog-Verhandlungen (Beratungen, zu denen Vertreter der drei am Gesetzgebungsverfahren beteiligte Institutionen zusammensetzen, Europäische Kommission, Rates der Europäischen Union sowie das Europäische Parlament) ersatzlos entfallen, so dass nunmehr auch kürzere Befristungen als zwei Jahre möglich wären. Vor dem Hintergrund der unabhängigen Aufgabenwahrnehmung ist dies als **kritisch** anzusehen. Wer ständig fürchten muss, dass seine Bestellung nicht verlängert wird, dem wird es schwerfallen, im Interesse des Datenschutzes auch Positionen einzunehmen, die der Unternehmensleitung bzw. Fachabteilung unlieb sind. Dabei ist es unerheblich ob die Tätigkeit, Vollzeit oder Teilzeit durchgeführt wird. Eine

1225 *RA Jaspers, Andreas /RAin Reif, Yvette, LL.M.* RDV / Recht der Datenverarbeitung Heft 2/April 2016, 61.

Wiederernennung sollte möglich sein, zumindest nach dem aktuellen Stand der Gesetzeslage.

1.4.5 Aufgaben

Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

1. Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;
2. Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
3. Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35;
4. Zusammenarbeit mit der Aufsichtsbehörde;
5. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.

(2) Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

1.4.6 Abberufung

Der betriebliche Datenschutzbeauftragte kann bei Vorliegen bestimmter Voraussetzungen abberufen werden, die DS-GVO äußert sich hierzu im Gegensatz zum bisherigen BDSG nicht explizit, sondern stellt lediglich in negierender Weise klar, dass eine Wahrnehmung seiner Aufgaben jedenfalls kein Grund zur Abberufung sein kann.

Dieser Schutz ist wichtig für den Datenschutzbeauftragten, um auch im Konfliktfall mit der Geschäftsführung einen gesetzlichen Rückhalt zu haben.[1226]

1.4.7 Social-Media

In der Regel sind Datenschutz und Social-Media nicht miteinander vereinbar. Das Problem bei Facebook, Instagram und Co. sind die für die Nutzung der Plattformen erforderlichen Daten. Einerseits wird vor Beginn der Nutzung einer Plattform ein „Opt-In" Verfahren gefordert, im Anschluss allerdings alle persönlichen Daten freiwillig präsentiert. Darin werden in der Regel Informationen dargestellt, die dem gesunden Menschenverstand widersprechen würden. In einer Zeit, in denen das Thema „Klingelschilder" als möglicher Verstoß gegen Datenschutzrecht diskutiert wird, werden bereitwillig personenbezogene Daten über Rasse, Herkunft, sexuelle Vorlieben, Adresse, Arbeitgeber, Kopien des eigenen Personalausweises, Bilder der Kinder, Kennzeichen der selbst genutzten Fahrzeuge inkl. deren Versicherungen u.v.m. präsentiert. Es werden Themen gepostet wie bspw. „wir gehen morgen in Urlaub, unser Flieger geht um diese Uhrzeit und der Zielort ist…". Wie schwierig kann es in diesen Fällen noch sein, den Wohnort ausfindig zu machen, die Wohnung auszurauben und oder die Identität zu übernehmen. In einigen Fällen wurde, durch die Informationen über den Krankenhausaufenthalt eines Verwandten, die Identität eines nahen Verwandten verwendet, um Informationen aus dem Krankenhaus zu erhalten, die zur Planung des Mitarbeiters bzw. Mitarbeiterin bezüglich der Erstellung eines Dienstplanes benötigt wurden, verwendet. Wenn der Ausspruch, „das Internet vergisst nie" für eine Situation passt, dann für die Selbstdarstellung über die Plattformen der Sozialen Medien.

Zwischenzeitlich, im Wissen über die Macht der Sozialen Medien, sind die Unternehmen dazu übergegangen, das eigene Unternehmen auf diesen Plattformen zu präsentieren. Gerne werden durch derartige Maßnahmen so viele Informationen wie irgend möglich präsentiert. Das Recht auf das eigene Bild und die Möglichkeiten die dargestellten personenbezogenen Daten gelöscht zu bekommen und oder korrigiert zu wissen, ist in dieser Darstellungsvariante nicht einfach umsetzbar. Bilder und Daten können mit sehr einfachen Mitteln gespeichert, geteilt oder genutzt werden. In diesen Fällen ist es extrem

1226 *Schläger/Thode* (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, Stutz, S. 113 und 114, Rn. 84.

wichtig eine angemessene Planung vorzunehmen, die alle Eventualitäten berücksichtigt. Gleiches gilt für die Einwilligung der betroffenen Personen. Wer ist auf der Seite zu sehen? Handelt es sich um einen Mitarbeiter oder Mitarbeiterin oder gar um einen Kunden? Wurde hierzu ausdrücklich eine Einwilligung erklärt?

Mit Zugang zum Internet ist es aktuell möglich, durch ein Bild mögliche Verbindungen zu personenbezogenen Daten zu erhalten (bspw. Google Foto). Werden zusätzlich Daten wie Name, Stadt oder Arbeitgeber mitgeteilt, ist der Weg zu einem effektiven Profiling, Tür und Tor geöffnet.

Das bloße Präsentieren ist seit einiger Zeit nicht mehr ausschließliches Ziel einer Social-Media Plattform. Gerne wird die Interaktion zwischen den Nutzern, Webseiten, Social-Media Plattformen und Internetauftritten genutzt, um den Besuchern / Nutzern alle Möglichkeiten aufzuzeigen, wie eben die vollumfängliche Nutzungsmöglichkeit an allen Systemen teilnehmen zu können. Zu diesem Zweck ist es erforderlich, sogenannte Plug-Ins in das eigene System einzubinden. Das „liken“ und „Teilen“ auf Webseiten und oder Plattformen ist aktuell all Gegenwertig. Da bei Nutzung der Plug-In Schalter / Buttons Daten des Rechners, der diesen Vorgang vorgenommen hat, an den Betreiber bzw. Inhaber der Seite / Plattform übermittelt, ist dieses ein nicht unerhebliches Thema zur Datensicherung bzw. Datenschutz-Grundverordnung. Die Erfahrung der letzten Jahre lehrt allerdings, dass vor allem außerhalb Europas ansässige Anbieter wenig Rücksicht auf europäische Datenschutzvorgaben nehmen, so dass – trotz erweiterter Möglichkeiten der Datenschutzaufsichtsbehörden gegen Anbieter in Drittstaaten –Website-Betreiber die datenschutzrechtlichen Vorgaben kaum einhalten können.[1227]

Das OLG Düsseldorf hat sich aus diesem Grund mit sechs datenschutzrelevanten Fragen an den Europäischen Gerichtshof gewandt, um hier Klarheit zu erlangen. (vgl. Az.: I-20 U 40/16) Um derartige Probleme vermeiden zu können, kann es erforderlich sein, einen Einsatz von Plug-Ins im Social-Media Bereich anhand einer Erklärung zu formulieren. Eine Muster-Vorlage befindet sich im Anhang dieser Arbeit und dient lediglich als Muster. Die Vorlage muss, entsprechend den aktuell geltenden Gesetzen und Vorschriften, angepasst und überprüft werden.

1227 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, Lachenmann, S. 557.

1.4.8 Meldung einer Datenpanne

Als Datenschutzbeauftragter oder Verantwortlicher sind sie verpflichtet Datenschutzverstöße nach Art. 33 Datenschutz-Grundverordnung zu melden. Gleiches gilt für den Auftragsverarbeiter. Die Meldepflicht hat unmittelbar nach Eintritt einer Verletzung des Schutzes personenbezogener Daten zu erfolgen. Der Verantwortliche ist verpflichtet, Maßnahmen einzuleiten die einen Schaden verhindern oder sofern ein Schaden bereits entstanden ist, diesen umgehend und unverzüglich zu minimieren oder abzustellen. Die Art der Verletzung der personenbezogenen Daten ist dabei unerheblich. Hierzu ist ein Risikomanagement zu implementieren, dass das Ziel hat, mögliche Verletzungen bereits im Vorfeld auszuschließen. Alle Datenschutzbehörden bieten hierzu auf ihrer Webseite entsprechende Formulare an, die online ausgefüllt und versendet werden müssen. Die Meldefrist beträgt 72 Stunden. Weiterhin muss durch Abwesenheit des oder der Verantwortlichen gewährleistet sein, dass eine Vertretungsregelung existiert und auch aktiviert wird, sollte es zu einer Verletzung des Schutzes von personenbezogenen Daten kommen.

Nachfolgendes Formular stellt lediglich ein Muster dar, welches für den Fall der Nutzung an die Bedürfnisse des entsprechenden Unternehmens angepasst werden sollte.

Meldung einer Datenschutzverletzung nach Art. 33 DSGVO
Angaben zur betroffenen Organisation (Verantwortlicher)
Name (Pflichtfeld)
Organisation
Straße und Hausnummer
Postleitzahl
Stadt
Webseite
Name der Kontaktperson
Wer meldete den Vorfall
Name
Straße
Postleitzahl
Ort
E-Mail – Adresse
Telefonnummer
Verhältnis zur betroffenen Organisation

Angaben zum Vorfall	
Kategorie des Vorfalls (siehe die am häufigsten gemeldeten Datenschutzverletzungen) *In der Online Version dieser Arbeit befindet sich ein Drop-Down Menü anstelle der sieben Auswahlmöglichkeiten.*	
Postfehlversand	☐
Hackingangriffe/Malware/Trojaner	☐
E-Mail-Fehlversand	☐
Diebstahl eines Datenträgers	☐
Versendung einer E-Mail mit offenem Adressverteiler	☐
Verlust eines Datenträgers	☐
Fax-Fehlversand	☐
Zeitpunkt / Zeitraum des Verstoßes	
Datum und Uhrzeit der Feststellung des Verstoßes	
Sachverhalt	
Art der betroffenen Daten	
Wie wurde reagiert	
Ergriffene technische und organisatorische Maßnahmen	
Anzahl der Betroffenen	
Anhang, sofern vorhanden und relevant (optional)	

Abbildung 25: Formular zur Meldung einer Datenschutzverletzung (Panne)

1.5 Verhängte Bußgelder (auszugsweise)

Ist die Geschäftsleitung und sind die **MitarbeiterInnen** entsprechend der Datenschutz-Grundverordnung **sensibilisiert** oder besteht nach wie vor der **Gedanke**, das ist alles **nicht so schlimm**? Wie steht es mit der technischen Umsetzung, insbesondere mit dem Umgang personenbezogenen Daten?

Die am häufigsten gemeldeten Datenschutzverletzungen seit Einführung der Datenschutz-Grundverordnung können nachfolgender Tabelle entnommen werden.

PLATZ	ART DER MELDUNG
1	Postfehlversand
2	Hackingangriffe / Malware / Trojaner
3	E-Mail-Fehlversand
4	Diebstahl eines Datenträgers
5	Versendung einer E-Mail mit offenem Adressverteiler
6	Verlust eines Datenträgers
7	Fax-Fehlversand

Abbildung 26: Die am häufigsten gemeldeten Datenschutzverletzungen[1228]

Die Aufsichtsbehörden haben seit der Einführung im Jahr 2016 und deren tatsächlicher Umsetzung, im Jahr 2018, mehrere, im Vergleich zum ehem. Bundesdatenschutzgesetz, **erhebliche Bußgelder** verhängt. Dieses geschah aus den unterschiedlichsten Gründen, wie nachfolgend aufgeführt wird:

1228 *Pressestelle, Datenschutz und die Informationsfreiheit Baden-Württemberg*, DATENSCHUTZVERLETZUNGEN BEREITEN ZUNEHMEND SORGE!, Die am häufigsten gemeldeten Datenschutzverletzungen, Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/07/PM-Datenschutzverletzungen-bereiten-zunehmend-Sorge-30.07.2019.pdf.

1.5.1 Deutsche Wohnen SE

Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft

Am 30. Oktober 2019 hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit gegen die **Deutsche Wohnen SE** einen Bußgeldbescheid in Höhe von rund 14,5 Millionen Euro wegen Verstößen gegen die Datenschutz-Grundverordnung (DS-GVO) erlassen. Bei Vor-Ort-Prüfungen im Juni 2017 und im März 2019 hat die Aufsichtsbehörde festgestellt, dass das Unternehmen für die **Speicherung personenbezogener Daten** von Mieterinnen und Mietern ein **Archivsystem** verwendete, das **keine Möglichkeit** vorsah, **nicht mehr erforderliche Daten zu entfernen**. Personenbezogene Daten von Mieterinnen und Mietern wurden gespeichert, ohne zu überprüfen, ob eine Speicherung zulässig oder überhaupt erforderlich ist. In begutachteten Einzelfällen konnten daher teilweise Jahre alte private Angaben betroffener Mieterinnen und Mieter eingesehen werden, ohne dass diese noch dem Zweck ihrer ursprünglichen Erhebung dienten. Es handelte sich dabei um **Daten zu den persönlichen und finanziellen Verhältnissen der Mieterinnen und Mieter, wie z. B. Gehaltsbescheinigungen, Selbstauskunftsformulare, Auszüge aus Arbeits- und Ausbildungsverträgen, Steuer-, Sozial- und Krankenversicherungsdaten sowie Kontoauszüge**[1229]

Das Archivsystem der Deutschen Wohnen SE hatte keine Möglichkeiten vorgesehen, die erhobenen personenbezogenen Daten zu löschen und somit den Vorgaben der Datenschutz-Grundverordnung sowie der Berliner Datenschutzbehörde nachzukommen. Dieses obwohl die Datenschutzbehörde im Jahr 2017, in einer ersten Überprüfung, **explizit** darauf hingewiesen hatte. Die Nachprüfung im Jahr 2019 ergab, dass das Unternehmen die Datenbestände nicht bereinigt hatte. Hier galt der Grundsatz, „Privacy by Design“ nach Art. 5 und 25 der Datenschutz-Grundverordnung. Die technische Gestaltung der verwendeten Systeme zur Erfassung der personenbezogenen Daten hätte die Möglichkeit der Bereinigung bzw. Löschung (Recht auf Vergessenwerden) hergeben müssen.

1229 Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft, Berliner Beauftragte für Datenschutz und Informationsfreiheit, Berlin, Pressemitteilung vom 05.11.2019.

1.5.2 1&1

Auf Grundlage des Art. 32 DS-GVO wurde das Unternehmen 1&1 im Dezember 2019 mit einem Bußgeld in Höhe von 9,5 Millionen Euro belegt. Hintergrund war, dass durch die Hotline des Unternehmens eine unberechtigte Person „weitreichende Informationen" zu weiteren personenbezogenen Daten verhältnismäßig einfach erhalten hat. Trotz der Einsicht sowie uneingeschränkte Zusammenarbeit mit der Datenschutzbehörde wurde 1&1 mit der oben genannten Bußgeldhöhe belegt. Das Unternehmen kündigte an, gegen den Bescheid klagen zu wollen.

1.5.3 British Airways

Ebenfalls auf Grundlage des Art. 32 DS-GVO wurde die britische Fluggesellschaft British Airways mit einer Geldstraße in Höhe von 203 Millionen GBP (183 Millionen Euro) belegt. Die Aufsichtsbehörden haben dieses mit den unzureichenden Sicherheitsvorkehrungen begründet. Durch einen gezielten **Cyber-Angriff** konnte die Webseite der British Airways „gehackt" werden. Der Nutzerverkehr wurde in Folge des Angriffs auf eine „**Fake-Seite**" umgeleitet, wodurch Kundendaten über einen Zeitraum von mehreren Monaten, völlig unbemerkt gesammelt werden konnten. Schätzungen zufolge seien rund 500.000 Kunden davon betroffen gewesen. Hintergrund für die Höhe des Bußgeldes war die völlig unzureichenden Sicherheitsvorkehrungen sowie die abenteuerliche Anzahl an Kundendaten.

1.5.4 TIM SpA

Von Anfang 2017 bis Anfang 2019 wurden mehrere hunderte Beschwerden über unerwünschte Werbeanrufe des italienischen Telekommunikationsanbieters, TIM, an die Aufsichtsbehörden gemeldet. TIM hatte mit der Durchführung ein externes Call-Center beauftragt. Laut Untersuchungen der Aufsichtsbehörden, lägen für die millionenfachen Anrufe keine Einwilligung gemäß Datenschutz-Grundverordnung nach Art. 5 Abs. 1 lit. a, b und e sowie Art. 7 Abs. 1 und 2 DS-GVO vor. In einigen Fällen wurde der Kontaktaufnahme ausdrücklich widersprochen. Darüber hinaus wurde die unrichtige und intransparente Information zur Datenverarbeitung, bezogen auf die Apps (App – Application) des Unternehmens, beanstandet. Abschließend wurden die eingesetzten IT-Systeme beanstandet. Diese entsprachen ebenfalls nicht den Anforderungen nach Art. 25 DS-GVO (**Privacy by Design**).

TIM wurde mit einem Bußgeld in Höhe von 27 Millionen Euro belegt, zahlbar innerhalb 30 Tagen, verbunden mit einer Auflage sowie 20 Anweisungen, die durch die App erhaltenen personenbezogenen Daten nicht zu Werbezwecken zu nutzen.

1.5.5 Google Frankreich

*"On 21 January 2019, the **CNIL's**(**C**ommission **N**ationale de l'**I**nformatique et des **L**ibertés) restricted committee imposed a financial penalty of 50 Million euros against the company GOOGLE LLC, in accordance with the **G**eneral **D**ata **P**rotection **R**egulation (**GDPR**), for lack of transparency, inadequate information and lack of valid consent regarding the ads personalization".*[1230]

Die nationale Datenschutzkommission Frankreichs verhängte gegen das Unternehmen Google Frankreich ein Bußgeld in Höhe von 50 Millionen Euro. Der Erlass erfolgte mangels Transparenz, unzureichender Informationen und fehlender Einwilligung in Bezug auf die Personalisierung von Werbeformaten. Hierbei handelte es sich um einen Verstoß gegen die Informationspflicht über die Art und Weise der Nutzung personenbezogener Daten. Somit wurde geltendes Recht verletzt: Art. 4 Abs. 11, Art. 13, Art. 14, Art. 6 sowie Art. 5 DS-GVO.

Randbemerkung: Vor Einführung der Datenschutz-Grundverordnung betrug in Frankreich die maximale Bußgeldhöhe 150.000 Euro.

1.5.6 La Liga de Fútbol Profesional

Die Ausrichter der höchsten spanischen Fußball-Ligen sind von spanischen Datenschützern mit einem **Bußgeld** mit **250.000 EUR** belegt worden. Der Ausrichter **L**iga Nacional de **F**útbol **P**rofesional (**LFP**), auch La Liga genannt (vergleichbar mit der deutschen DFL) hatte in einer von ihr bereitgestellten App nicht klar dargelegt, dass diese App automatischen Zugriff **auf Positionsdaten** sowie das Mikro des Smartphones gewährt. Diese unsichtbaren Funktionen wurden von Seiten der Organisation „La Liga" installiert, um unlizenzierte Übertragungen von Spielen, die ausschließlich in Pay-TV zu sehen sind, aufzuspüren. Während der Fußball Übertragungen wurden Umgebungsgeräusche registriert und überprüft, um in der Folge beispielsweise

1230 The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, https://www.cnil.fr/en/node/287.

Fußballübertragungen in Gaststätten zu orten, die keine offizielle Übertragungslizenz hatten.[1231]

Die spanischen Aufsichtsbehörden sahen in dieser Maßnahme einen klaren Verstoß gegen das Transparenzgebots nach Art. 5 Abs. 1 lit. a sowie Art. 7 Abs. 3 DS-GVO

1.5.7 Universitätsmedizin der Johannes-Gutenberg-Universität Mainz

Der Bescheid wurde am 03.12.2019 zugestellt. Damit ist die Universitätsmedizin der Johannes-Gutenberg-Universität Mainz die erste Organisation in öffentlicher Trägerschaft in Deutschland, gegen die aufgrund eines Verstoßes gegen die Datenschutz-Grundverordnung ein Bußgeld verhängt wurde.

Die Geldbuße in Höhe von 105.000 EUR beruhte auf Verstößen im Zusammenhang mit einer Patientenverwechslung bei der Aufnahme eines Patienten. Die Verwechslung hatte eine **falsche Rechnungsstellung** zur Folge und offenbarte **strukturelle technische und organisatorische Defizite** des Krankenhauses beim **Patientenmanagement**. Das Bußgeld ist rechtskräftig. (vgl. Art. 9 und Art. 6 DS-GVO)

1.5.8 Österreichische Post

Die österreichische Post hat aufgrund der Sammlung von Daten zur Parteiaffinität, im Jahr 2019 ein Bußgeld in Höhe von 18 Millionen Euro auferlegt bekommen. Obwohl das Urteil aktuell noch nicht rechtskräftig ist, muss die Post mit einem erheblichen Bußgeld rechnen, da das Sammeln von personenbezogenen Daten ohne einen direkten Bezug zur Aufgabe der Post, ein Bußgeld nach sich ziehen kann. Die Höhe der Strafe richtet sich nach der Anzahl der betroffenen Personen und wird zusätzlich mit 10 % Verfahrenskosten beaufschlagt, bezogen auf das ausgesprochene Bußgeld. (vgl. Art. 9 DSGVO sowie Art. 5 Abs. 1 lit. a DSGVO)

1231 *Compliance Essentials GmbH, Lochhamer Str. 31, 82152 München-Planegg,* Bußgelddatenbank, https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php.

1.5.9 National Revenue Agency (Nationale Finanzbehörde Bulgariens)

Der Nationalen Finanzbehörde Bulgariens wurde vorgeworfen keinerlei technische und organisatorische Maßnahmen aufgesetzt zu haben, um Datenschutzrechtliche Verstöße zu unterbinden. Dies führte dazu, dass Unbekannte Zugriff auf personenbezogene Daten von über 6 Mio. Personen erlangten. Hierbei handelte es sich um Namen, persönliche Identifikationsnummern und Adressen, Telefonnummern, E-Mail-Adressen und anderen Kontaktdaten sowie Daten aus den jährlichen Steuererklärungen. Das Bußgeld in Höhe von umgerechnet über 2,6 Mio. Euro ist die bisher höchste ausgesprochene Summe in Bulgarien (vgl. Art. 32 DSGVO)[1232]

1.5.10 Vueling Airlines S.A.

Die spanische Datenschutzbehörde hat die Airline Vueling Airlines S.A. abgemahnt und mit einer Strafzahlung von 30.000 Euro belegt. Hintergrund war ein, den europäischen Regelungen der DS-GVO, nicht konformer Cookie-Banner. Bei Aufruf der offiziellen Webseite der Airline erscheint ein Cookie-Banner der den nachfolgenden Text (Übersetzung aus dem Spanischen):

Wir verwenden Cookies, um Ihre Präferenzen zu speichern, Nutzungsstatistiken zu erstellen und Werbeangebote basierend auf Ihren Browsing-Gewohnheiten an Sie zu senden. Wenn Sie weitersurfen, ***nehmen wir an****, dass Sie deren Verwendung akzeptieren. Weitere Informationen diesbezüglich erhalten Sie in unseren Cookie-Bestimmungen.*

Der EuGH hat zu voreingestellten Einwilligungen im Oktober 2019 (Az. C-673/17) Stellung genommen. Die Einwilligung durch voreingestellte Auswahlkästchen ist somit nicht zulässig. In Spanien gilt dieses Prinzip im Bereich des E-Commerce bereits seit 2002. (vgl. hierzu Art. 5 DS-GVO)

1232 *Compliance Essentials GmbH, Lochhamer Str. 31, 82152 München-Planegg* (Hrsg.), Bußgelddatenbank, https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php 2020, https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php.

1.5.11 Facebook

Das bis dato höchste **Bußgeld,** für ein Datenschutzvergehen, wurde dem Unternehmen Facebook auferlegt. **Facebook** musste trotz einer **Einigung** mit den US-Behörden ein Bußgeld in Höhe von **5 Milliarden Euro** entrichten. Begründet wurde dies mit mehrfachen Verstößen gegen **FTC**-Datenschutzanordnungen (FTC – ***F***ederal ***T***rade ***C***ommission) aus dem Jahr 2012 sowie 2018, bei welchen Facebook pflichtwidrig über die Schutzmöglichkeiten von Nutzerdaten getäuscht hatte.[1233]

Ausgehend von den Artikeln der Datenschutz-Grundverordnung wären bis zu 4 % des letztjährigen Konzernumsatzes möglich gewesen. Eine Übersicht über die verhängten Bußgelder kann im Internet problemlos abgerufen werden.[1234]

1233 *Gruenwald Henderson, Juliana, Kaplan Peter, Office of Public Affairs*, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, FTC settlement imposes historic penalty, and significant requirements to boost accountability and transparency, FTC - Federal Trade Commission July 24, 2019, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

1234 Dsgvo-portal.de, Vgl. https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php, Bußgeld-Datenbank 2020.

1.6 Aktuelle Situation durch die Corona Krise (Covid. 19)

Bei den oben aufgeführten Fragen handelt es sich lediglich um eine aktuelle auf die Situation bezogene Aufzählung einiger Fragen zum Thema Datensicherheit. Es ist aber hierbei zu beachten, dass die aktuelle „**Ausnahmesituation**“ nicht benutzt werden sollte, um die mühsam erworbenen **Grundrechte** wieder abzubauen. Die Problematik besteht in der Überprüfung der während der „Corona Pandemie“ gesammelten personenbezogenen Daten. Die aktuellen Notstandgesetze weichen aus den bekannten Gründen die Grundrechte der Bevölkerung auf. Es ist allerdings zu prüfen, wie weit dieses gehen kann und was technisch möglich ist. Es ist technisch ohne Probleme machbar, dass die Mobilfunkanbieter in Deutschland durch ein Überprüfen der Mobilfunkdaten, erfassen können, ob die jeweiligen Nutzer in ihrem Haus / Wohnung bleiben (Ausgangssperre) oder ob diese unterwegs sind. Diese Maßnahme wird aktuell von der österreichischen Regierung durchgeführt.

„eine Auswertung der “Bewegungsströme“ von Handynutzern habe ergeben, dass sich Bewegungen im Vergleich zur vergangenen Woche fast halbiert hätten. Die Daten stammen von A1 - mit fast fünfeinhalb Millionen Handykunden ist das der größte Mobilfunkanbieter des Landes. Das Unternehmen habe die Daten von sich aus der Regierung angeboten, sagt Sprecherin Livia Dandrea-Böhm. Aus den Daten könne man keine Bewegungsprofile für einzelne Personen erstellen, sondern lediglich für Gruppen von 20, 40, oder 60 Personen - also immer in 20er-Schritten - betont Dandrea-Böhm. "Es ist alles datenschutzrechtlich konform, telekommunikationsgesetzeskonform und auch vom TÜV datenschutzrechtlich geprüft“ [1235]

Problematisch könnte die Situation werden, wenn die österreichische Regierung nach Aufhebung der Ausgangssperre die Daten nicht datenschutzkonform löscht. Die Technik und Datenbank zur Speicherung und Nutzung der Bewegungsdaten, und somit personenbezogenen Daten, zur Überwachung wäre ja bereits vorhanden. Hier kann ganz aktuell der Ausdruck zu den Anfängen der Datenschutz-Grundverordnung, „**wer überwacht eigentlich die Überwacher?**“ angeführt werden.

1235 *Srdjan Govedarica, ARD-Studio Wien von*, Österreich überwacht Handydaten, Coronavirus (Covid 19) 18.03.2020, 16:25 Uhr, https://www.tagesschau.de/investigativ/handyueberwachung-oesterreich-101.html.

Spanien benutzt in der aktuellen Krise, **Drohnen**, um die Bevölkerung nach Hause zu bekommen und die Ausgangssperre kontrollieren zu können.[1236] Spanien hat mit der aktuellen Pandemie sehr stark zu kämpfen und das Verständnis für alle erforderlichen bzw. verhältnismäßigen Maßnahmen ist zu verstehen. Datenschutzrechtlich ist die Situation etwas differenzierter zu betrachten. Drohnen sind mit hochauflösenden digitalen Kameras und leistungsfähigen Speichermedien ausgestattet. Spanien setzt darüber hinaus Techniken ein, die es ermöglichen, über die Drohnen eigene Lautsprecher Durchsagen zu tätigen. Es besteht somit immer die Möglichkeit diese gespeicherten Daten zur späteren Strafverfolgung verwenden zu können. Eine einmal aufgebaute und gepflegte Datenbank möchte man nicht missen wollen.

In Deutschland sind bereits Gespräche im Gange die eine „freiwillige" Nutzung einer sogenannten „Corona-App" vorschlagen. Dadurch soll die Möglichkeit geschaffen werden, den Kontakt zu einer infizierten Person nachvollziehen zu können.

Am 16.06.2020 wurde die Corona (Covid-19) Warn-App zum Download bereitgestellt. Die offizielle deutsche Warn-App soll im Kampf gegen den Virus unterstützend agieren. Die App soll NutzerInnen benachrichtigen, wenn sich diese in der Nähe einer positiv getesteten Person aufgehalten hat / haben. Diese Maßnahme soll die Nachverfolgbarkeit möglicher Infektionsketten ermöglichen. Dazu wird der Kurzstreckenfunk, Bluetooth anstelle einer GPS-Variante, eingesetzt. Gemessen wird, ob sich AnwenderInnen über einen Zeitraum von 15 Minuten oder länger näher als ungefähr 2 Meter gekommen sind. Zur Messung werden in regelmäßigen Abständen (alle zwei bis fünf Minuten) anonymisierte Identifikationsnummern übertragen. Wird ein Anwender positiv auf das Virus getestet, erhält der Nutzer, der die oben abgegebene Zeit in der unmittelbaren Nähe der infizierten Person verbracht hat, eine Warnung über die App. Positiv getestete Personen müssen sich in der Folge bei der Hotline für Infektionsmeldungen melden. Nutzer sollen zusammen mit einem positiven Testergebnis auch einen QR-Code erhalten, der durch die App eingescannt werden kann. So findet die Bestätigung über eine tatsächliche Infizierung statt. Exakt in diesem Bereich sehen Fachleute die Schwäche des Systems. Bei einem persönlichen Kontakt über die Hotline werden unterschedliche Daten ausgetauscht. Diese werden in einer Datenbank erfasst und für die Erstellung der QR-

1236 *ORF - österreichischer Rundfunk,* Drohnen zur Überwachung der Ausgangssperre in Spanien, https://orf.at/stories/3158224/.

Codes verwendet werden. Bei der Meldung wird ein Abgleich über die Mobilfunknummer vorgenommen, die bereits zu den **personenbezogenen Daten** zählt. Nach Art. 35 DS-GVO müssen alle Datenverarbeiter vor riskanter Verarbeitung eine Datenschutz-Folgenabschätzung durchführen. Bei der Corona-App ist dieses definitiv der Fall, da hier Unmengen an Gesundheitsdaten verarbeitet werden.

Als weitaus Problematischer wird die Freiwilligkeit des Einsatzes einer Corona-Warn-App gesehen. Es ist durchaus möglich, dass unterschiedliche Situationen nur unter dem Gesichtspunkt des Einsatzes einer solchen App erlaubt werden, bspw. unproblematische Rückkehr an den Arbeitsplatz o.ä.. Darüber hinaus ist die App nicht in der Lage zu bestimmen, ob eine in „Selbst - Quarantäne“ befindliche Person, die sich regelmäßig in einem separaten Bereich (durch Türen und Wände abgetrennt) aufhält aber keinen Abstand > 2 Meter einhält, keinen persönlichen Kontakt hatte. Bei einem positiven Befund der „anderen Person“ wird hier grundlos ein falsch positives Ergebnis angenommen.[1237]

Aufgrund datenschutzrechtlicher Bedenken hinsichtlich eines Einsatzes der Corona-App wurde der Quellcode[1238] der App offengelegt. Darin enthalten sind die Code-Zeilen der App aus denen Programmierer und Fachleute die Funktion der Corona-App bestimmen können. Hierbei handelt es sich um eine finale Version, welche in der praktischen Anwendung noch getestet werden muss. Es ist zu hoffen, dass keine erheblichen Änderungen durch mögliche Updates eingesetzt werden, sondern nur eine Fehlerbeseitigung vorgenommen wird. Zum jetzigen Zeitpunkt wird die Corona-Warn-App als datenschutzrechtlich unbedenklich eingestuft.

Selbst bei einer dezentralen Speicherung der Daten besteht die Möglichkeit, dass der Mobiltelefonhersteller (bspw. Apple, Samsung oder Google) Informationen über das Verhalten der Nutzerinnen und Nutzer erhält, um damit ein Profil erstellen zu können.

1237 *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung*, Datenschutz-Folgenabschätzung für die Corona-App, Version 1.6 - 29. April 2020, https://www.fiff.de/dsfa-corona.

1238 *Informatik-verstehen.de,* Der Quellcode, auch bekannt als Quelltext oder Source Code, ist eine Textdatei im Standard-ASCI-Format, die alle Befehle und Anweisungen eines mit einer höheren Programmiersprache erstellten Programms enthält, https://www.informatik-verstehen.de/lexikon/quellcode/.

Wegen der Verarbeitung personenbezogener Gesundheitsdaten, ist zudem besondere Vorsicht geboten. Weil nur Daten derjenigen Personen übertragen werden, die als **infiziert** diagnostiziert wurden. Dabei handelt es sich bei den übertragenen Daten um Gesundheitsdaten. Ihre Verarbeitung ist nach Art. 9 DS-GVO nur in besonders eingeschränkten Maße zulässig. Eine mögliche Rechtsgrundlage ist die Einwilligung der Betroffenen, die jedoch nur bei freiwilliger Erteilung wirksam ist. Alternativ könnten gesetzliche Grundlagen geschaffen werden. Das Infektionsschutzgesetz bietet bisher nach überwiegender Ansicht keine Rechtsgrundlage dafür.[1239]

Der Verhältnismäßigkeitsgrundsatz ist in Deutschland Bestandteil der aktuellen Grundrechte sowie der regelmäßigen Rechtsprechung so auch im Datenschutzrecht. Art. 20, 28 Abs. 1 des Grundgesetzes besagt, „dass ein Eingriff erforderlich, geeignet und verhältnismäßig im engeren Sinne sein muss“. Er gilt insbesondere für alle Eingriffe der öffentlichen Hand in verfassungsmäßig geschützte Rechte der Betroffenen.[1240]

Zum aktuellen Zeitpunkt erklärt der Bundesdatenschutzbeauftragte, der die Situation des Datenschutzes regelmäßig beobachtet, dass die **aktuelle Datenverarbeitung**, datenschutzrechtlich **vertretbar** sei.

Nach Ende der Einschränkungen des öffentlichen Lebens sollte unbedingt überprüft werden, ob und wie die Maßnahmen im Zuge der Rückführung in die „Normalität“ wieder abgeschafft wurden. Nur derartige Maßnahmen können dahingehend Gewissheit bringen, dass die schwer erkämpften Grundrechte, auf Schutz der personenbezogenen Daten, weiterhin Bestand haben.

1239 *Datenschutzbeauftragter-info.de*, Die Corona App – Risiken und Nebenwirkungen, Corona - App Risiken, https://www.datenschutzbeauftragter-info.de/die-corona-app-risiken-und-nebenwirkungen/.

1240 Grundgesetz für die Bundesrepublik Deutschland, Vgl. Art. 20, 28 Abs. 1 GG sowie Gabler Wirtschaftslexikon, "Verhältnismäßigkeit".

2 Fazit

Der Schutz personenbezogener Daten ist ein Grundrecht, welches es unter allen Umständen zu schützen gilt. Lange Zeit wurde der „sorglose“ Umgang mit dem wichtigsten Gut des 21 Jahrhunderts toleriert. Obwohl bereits lange Zeit thematisiert wurde der **tatsächliche** Schutz erst mit Einführung der Datenschutz-Grundverordnung aktiviert.

Die Datenschutz-Grundverordnung ist mit seinen 99 Artikeln und den dazugehörigen 173 Erwägungsgründen ein recht umfangreiches Werk geworden. Die theoretischen Ausführungen wurden, entgegen den Anforderungen der Datenschutz-Grundverordnung, wenig verständlich, nicht besonders transparent und vor allem nicht in besonders einfacher Sprache verfasst. Die Umsetzung der Datenschutz-Grundverordnung hatte im Vorfeld für erhebliche Unruhe in allen Bereichen, insbesondere in den Unternehmen, die diese in der vorgegebenen Zeit umzusetzen hatten, gesorgt. Im Gegensatz zum Bundesdatenschutzgesetz (alte Fassung), welches immer wieder gerne als „zahnloser Tiger“ bezeichnet wurde, hat die Datenschutz-Grundverordnung ein weit umfangreicheres Sortiment an Anforderungen sowie Sanktionen aufgefahren. Verstöße werden, wie die kurze Liste der Bußgeldbescheide eindrücklich aufzeigt, rigoros geahndet. Der Aufwand lohnt sich, wie aus den auszugsweise verhängten Bußgeldbescheiden aus dem Unterpunkt 1.5 (Teil. 3) der Handlungsempfehlungen dieser Arbeit, entnommen werden kann.

In der Europäischen Union sind, auch nach einem Ausstritt Großbritanniens, mehr als 24,97 Millionen Unternehmen (Deutschland 2,88 Millionen) gemeldet.[1241] Von der Datenschutz-Grundverordnung betroffenen Unternehmen, mit Sitz in der Europäischen Union, mussten die Datenschutz-Grundverordnung bis zur Einführung im Mai 2018 umgesetzt haben. Die tatsächliche Einführung fand eigentlich am 27. April im Jahr 2016 statt. Aufgrund der Komplexität der Verordnung wurde eine zweijährige Übergangszeit eingeräumt, die die betroffenen Unternehmen dazu nutzen sollten, die Einführung planmäßig und adäquat umsetzen zu können. Aus eigener Erfahrung ist anzuführen, dass

1241 -*Eurostat*- (Hrsg.), Wichtigste Variablen der Unternehmensdemografie, Online Datencode: TIN00170, letzte Aktualisierung 12.03.2020 Stand 2017.

einige Unternehmen erst einige Monate vor der „Scharfschaltung“ der Datenschutz-Grundverordnung mit der Einführung begonnen hatten. In einem bekannten Fall wurde der (Konzern-) Datenschutzbeauftragte erst am 24.05.2018 angestellt und mit der konzernweiten Betreuung beauftragt.

Die Umsetzung der Datenschutz-Grundverordnung in ein „lebendes“ Unternehmen einführen zu wollen, benötigte einiges an Arbeit. Alle Unternehmensbereiche mussten sich im ersten Schritt der Analyse aller Abläufe widmen. Mit einer ehrlichen Bestandsaufnahme ausgestattet musste ein Plan generiert werden, der zum Ziel hatte, die Datenschutz-Grundverordnung einzuführen. Die gewonnen Daten konnten darüber hinaus zur Analyse und Anpassungen der vorhandenen Unternehmensstrukturen verwendet werden. Wie die Umsetzung im Detail durchgeführt werden konnte bzw. kann ist aus dem Teil. 2 dieser Arbeit zu entnehmen. Obwohl die Einführung in ein Parkhausunternehmen beschrieben wurde, können die Daten ebenfalls für die generelle Analyse / Nutzung sowie Einführung verwendet werden. Hierzu wurden die betroffenen Abteilungen sowie die möglichen Berührungspunkten weitestgehend erfasst und beschrieben.

Bei der Einführung handelte es sich **nicht** um einen einmaligen Vorgang. Der gesamte Umgang mit personenbezogenen Daten muss sowohl permanent hinterfragt als auch in aller Regelmäßigkeit überprüft werden. Selbst bei der Anschaffung einer neuen Software muss die Umsetzbarkeit bzw. Nutzbarkeit des Systems in Bezug auf die Datenschutz-Grundverordnung überprüft werden. Es obliegt der Verantwortung der oder den verantwortlichen Personen hier bereits in der Planungsphase beratend zur Seite zu stehen.

In der Einführungsphase der Datenschutz-Grundverordnung wurden unzählige „sogenannte“ Profis aktiv. Einige Gruppen haben ein Geschäft daraus gemacht, mögliche Fehler in der Datenschutzerklärung der jeweiligen Webseiten, zu finden, um diese gewinnbringend abmahnen zu können. Andere wiederum konstruierten und vermarkteten Muster-Vorlagen für alles und jeden Zweck. In meinen Recherchen konnte ich viele sehr positive Anbieter und wirklich professionelle Unterstützung erfahren. Leider nutzen einige windige Anbieter die Unwissenheit der Unternehmen sowie der verantwortlichen Personen hemmungslos aus. Bei der Einführung eines derart komplexen Themas und dem Wissen darüber, dass im ersten Schritt viel Unsicherheit herrschte, wurden einige nicht unerhebliche Fehler gemacht. In der Folge mussten professionellen Betreuer / Unternehmen für Datenschutz sowie spezialisierte Kanzleien u.a. die Scherben aufkehren

und eine „echte“ Umsetzung betreuen. Anhand der aktuell vorliegenden Bußgeldbescheide sowie den noch anhängigen Verfahren ist davon auszugehen, dass längst nicht alle betroffenen Unternehmen die Datenschutz-Grundverordnung vollumfänglich umgesetzt haben. Wie in der Einleitung dargelegt, hat die Bitcom Research GmbH im September 2019 eine Studie über den Erfolg bezüglich der Umsetzung der Datenschutz-Grundverordnung durchgeführt. Demnach hat die deutsche Wirtschaft immer noch mit der Umsetzung der Datenschutz-Grundverordnung zu kämpfen. Fast eineinhalb Jahre nach Geltungsbeginn haben zwei Drittel der Unternehmen (67 %) die neuen Datenschutzregeln mindestens zu großen Teilen umgesetzt. Im Umkehrschluss bedeutet dieses allerdings, dass 33 % die Datenschutz-Grundverordnung noch nicht oder unzureichend umgesetzt haben. Da die Unternehmen per Datenschutz-Grundverordnung verpflichtet sind Datenschutzverfehlungen zu melden, kann dieses, je nach Schwere der Verfehlung, zu Bußgeldverfahren führen.

Das aktuelle Urteil des **Eu**ropäischen **G**erichts**h**of (**EuGH** Rechtssache C-673/17) hat mit seinem Urteil zum Thema Cookies nicht eben zur Beruhigung beigetragen. Die Anforderungen an Webseitenbetreiber steigen in ungeahnte Sphären auf. Kritische Stimmen beanstanden den nicht mehr vorhandene Praxisbezug. Als grobe Zusammenfassung ist anzuführen, dass für die Speicherung und Abrufen von Cookies auf dem Rechner des Besuchers einer Webseite jeweils eine Einwilligung erforderlich sein soll. Die voreingestellten Kästchen seien nicht ausreichend. Allerdings existieren ebenfalls anderslautende Meinungen hinsichtlich des aktuellen Urteils, welche besagen, dass nicht in jedem Fall eine Einwilligung erfolgen muss. Auch hier ist das letzte noch nicht Wort gesprochen.

Im Anhang dieser Arbeit finden sich einige Muster-Vorlagen, zu den unterschiedlichsten Bereichen, die unter datenschutzrechtlichen Gesichtspunkten gerne genutzt werden können.

Im dritten Teil der vorliegenden Arbeit wurden die möglichen Auswirkungen ausgeführt. Dabei wurden diejenigen Punkte aufgeführt, die der Verfasser als „erwähnenswert“ erachtete. Hierzu wurden Handlungsempfehlungen für die Bereiche der Geschäftsleitung, Personal sowie IT vorgenommen. Aufgrund der Wichtigkeit der Datenschutzbeauftragten bzw. Verantwortlichen wurden hierzu ebenfalls Punkte aufgeführt, die eine Betreuung bzw. Neueinführung sowie Unterstützung ermöglichen sollen.

Die aufgeführten Bußgeldbescheide und Verstöße sollen die möglichen Auswirkungen anhand einiger weniger Fälle darlegen. Die dort aufgeführten Bußgelder ermöglichen einen kleinen, aber detaillierten Ausblick in die Möglichkeiten der Aufsichtsbehörden hinsichtlich der Ahndung von Datenschutzverstößen und den daraus resultierenden Bußgeldzahlungen. Obwohl gemäß der aktuellen Datenschutz-Grundverordnung weit höhere Bußgelder möglich gewesen wären, haben sich die nationalen Aufsichtsbehörden, in Teilen, noch zurückgehalten. Ob und wie lange dieser Umstand anhält, wird die Zukunft aufzeigen.

In der ursprünglichen Planung waren Befragungen / Interviews sowie die Abfrage entsprechender Erfahrungen aus der Einführung der betroffenen Unternehmen geplant. Da dieser Teil der Arbeit aktuell nicht vorgenommen werden kann, wurde der Fragebogen zur Nutzung im Anhang abgelegt. Alle erdenklichen Punkte, sowie der Möglichkeit freien Text einzutragen, wurden berücksichtigt. Unabhängig von der hier vorliegenden Arbeit wird der Fragebogen durch den Verfasser der Arbeit zur Anwendung gebracht und analysiert werden. Da die Daten des Verfassers der vorliegenden Arbeit dem **B**usiness **S**cience **I**nstitut (**BSI**) vorliegen, besteht die Möglichkeit, durch die verantwortlichen Personen des Instituts, Kontakt mit dem Verfasser aufzunehmen. Die Erkenntnisse aus den Befragungen / Interviews können, nach Aufarbeitung und Prüfung der Anfrage, gerne übermittelt werden.

Anhang

_Toc57465637

I. Zeitschriften

DuD, Datenschutz und Datensicherheit, ISSN: 1614-0702

ZD, Zeitschrift für Datenschutz, ISSN: 2192-5593

RDV, Recht der Datenverarbeitung, ISSN: 0178-8930

PingG, Privacy in Germany (Datenschutz- und Compliance), ISSN: 2197 – 1862

Datenschutz Praxis, www.datenschutz-praxis.de, ISSN: 1614-6867

NJW, Neue Juristische Wochenschrift, ISSN: 0341-1915

II. Literaturverzeichnis

Ad Legendum, Die Ausbildungszeitschrift aus Münster Juridicum, in AD Legendum AL 1/2018, 1.

Albrecht, Albrecht, PM v. 7.3.2013, abrufbar unter: https://www.gruen-digital.de/2013/03/eu-datenschutz-ministerrat-muss-beim-datenschutz-liefern/; vzbv, PM v. 25.11.2014, abrufbar unter: https://www.vzbv.de/pressemitteilung/eu-datenschutzverordnung-weichen-stellen-fuer-mehr-datenschutz-0. 07.03.2013.

Albrecht, Astrid, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Zugl.: Frankfurt am Main, Univ., Diss., 2003, 2003.

Albrecht, Jan Philipp, Datenschutzrecht, DSGVO mit BDSG, hrsg. von Spiros Simitis, Gerrit Hornung, Indra Spiecker Döhmann, NomosKommentar, 2019.

Albrecht, Jan Philipp/Jotzo, Florian, Das neue Datenschutzrecht der EU, Grundlagen, Gesetzgebungsverfahren, Synopse, 2017.

Amt für Veröffentlichungen, EUR-Lex - ai0032 - EUR-Lex Datum der letzten Überprüfung: 08/09/2015.

ARTIKEL-29-DATENSCHUTZGRUPPE, Artikel-29-Datenschutzgruppe Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev. 01, angenommen am 28. November 2017 - zuletzt überarbeitet und angenommen am 10. April 2018, Die

Arbeitsgruppe für die Wahrung der Rechte von Personen bei der Verarbeitung personenbezogener Daten eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Guidelines/WP259_LeitlinienFuerDieEinwilligung.html.

ARTIKEL-29-DATENSCHUTZGRUPPE, Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, WP 148, Angenommen am 4. April 2008 2008.

Assion, Simon, Kommentar Datenschutz-Grundverordnung, hrsg. von Sibylle Gierschmann, Katharina Schlender, Rainer Stentzel u.a., Comply, 2018.

Assion, Simon/Brüggemann, Sebastian, DSGVO, BDSG, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze: Kommentar, hrsg. von Martin Eßer, Philipp Kramer, Kai von Lewinski, 5. Aufl., Heymanns Kommentare, 2017.

Atztert, Michael/Buchmann, Antonia/Dietze, Lars, Heidelberger Kommentar, DSGVO/BDSG, Datenschutzgrundverordnung, Bundesdatenschutzgesetz, Heidelberger Kommentar, hrsg. von Rolf Schwartmann, Andreas Jaspers, Gregor Thüsing u.a., Heidelberger Kommentar, 2018.

Auffarth, Fritz/Kaiser, Heinrich/Heither, Friedrich/Engels, Gerd/Schmidt, Ingrid/Trebinger, Yvonne/Linsenmaier, Wolfgang, Betriebsverfassungsgesetz, Handkommentar, 29. Aufl. 2018.

Bäcker, Matthias, Datenschutz-Grundverordnung, Kommentar, hrsg. von Jürgen Kühling, Benedikt Buchner, 2017.

Bäcker, Matthias/Bergt, Matthias/Boehm, Franziska/Caspar, Johannes/Dix, Alexander, Datenschutz-Grundverordnung/BDSG, Kommentar, hrsg. von Jürgen Kühling, Benedikt Buchner, 2. Aufl., 2018.

Barth. A, HTTP State Management Mechanism, Standards Track, Internet Engineering Task Force (IETF), U.C Berkeley April 2011, https://tools.ietf.org/pdf/rfc6265.pdf.

BDSG_erste_Fassung_1977.

Becker, Ansgar, Corporate Compliance Checklisten, Rechtliche Risiken im Unternehmen erkennen und vermeiden, hrsg. von Karsten Umnuß, 3. Aufl., 2017.

Becker, Thomas/Krohm, Niclas/Braunmühl, Patrick von/Kuhnke, Michael/Bussche, Axel von dem/Grages, Jan-Michael/Roggenkamp, Jan Dirk/Hullen, Nils/Schreiber, Lutz/Jenny, Valerian/Stamer, Philine/Kamlah, Wulf/Wittmann, Jörn, DSGVO/BDSG, Kommentar zu

DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG, hrsg. von Kai-Uwe Plath, 3. Aufl., Juris, 2018.

Beck'scher Online-Kommentar Datenschutzrecht, Online Kommentar Datenschutzrecht, 01.02.2017 (zit. als *Bearbeiter* in Beck'scher Online-Kommentar Datenschutzrecht).

Bergmann, Benjamin, EU-Ministerrat reitet auf Trojanischen Pferden Richtung Datenschutzreform 11.3.2013, https://netzpolitik.org/2013/innen-und-justizminister-reiten-auf-trojanischen-pferden-richtung-datenschutzreform/.

Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft, Berliner Beauftragte für Datenschutz und Informationsfreiheit, Berlin, Pressemitteilung vom 05.11.2019.

Bitcom Research GmbH, Zwei Drittel der Unternehmen haben DS-GVO größtenteils umgesetzt, Berlin 17.09.2019, https://www.bitkom-research.de/de/pressemitteilung/zwei-drittel-der-unternehmen-haben-ds-gvo-groesstenteils-umgesetzt.

Brink ZD / Zeitschrift für Datenschutz Heft 2, 57.

Buhl, Samir/Frieling, Tino/Krois, Christopher/Malorny, Friederike/Münder, Matthias/Richter, Barbara/Schmidt, Laura, Der erwachte Gesetzgeber, Regulierung und Deregulierung im Arbeitsrecht, 2017.

Bundesamt für Sicherheit in der Informationstechnik, Krypto-Richtlinien, BSI aktualisiert Krypto-Richtlinien der Serie TR-02102, erhöhtes Sicherheitsniveau von 120 Bit ab 2023 20.03.2017, https://www.bsi.bund.de/DE/Presse/Pressemitteilugen/Presse2017/Aktualisierte_Krypto-Richtlinien_TR–02102_20032017.html).

Bundesverfassungsgericht/Senat, 1., BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83 - Rn. (1 - 215), http://www.bverfg.de/e/rs19831215_1bvr020983.html.

Bußgeldverfahren gegen H&M (Hennes & Mauritz), Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Pressemitteilung vom 26.01.2020, https://datenschutz-hamburg.de/medienbildung_news/h_m/.

Buttarelli, Giovanni, Meeting the challenges of big data, A call for transparency, user control, data protection by design and accountability 07.2015, https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf.

b-wise GmbH, Wofür braucht es eine SWOT-Analyse, https://www.business-wissen.de/hb/wofuer-braucht-es-eine-swot-analyse/.

Byers, Philipp, Mitarbeiterkontrollen, Praxis im Datenschutz und Arbeitsrecht, 2016.

Caldarola, Maria Cristina/Schrey, Joachim, Big Data und Recht, Einführung für die Praxis, 2019.

CIPL (o. Fußn. 4), S. 4; Kuner/Cate/Millard/Svantesson/Lynskey, IDPL 2015, 95, 96.

Compliance Essentials GmbH, Lochhamer Str. 31, 82152 München-Planegg (Hrsg.), Bußgelddatenbank, https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php 2020, https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php.

Conseil de l'Europe, SEV 181 - Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr.

CZERNIK, AGNIESZKA, IP-Adressen – Funktion, Aufbau, Tracking, IP-Adresse - Internet Protokoll Adresse, https://www.datenschutzbeauftragter-info.de/ip-adressen-funktion-aufbau-tracking/.

Datenschutzbeauftragter-info.de, Datenschutzschulung – Mitarbeiter sensibilisieren, ohne zu langweilen, Die Schulungen müssen nicht langweilig sein!, https://www.datenschutzbeauftragter-info.de/datenschutzschulung-mitarbeiter-sensibilisieren-ohne-zu-langweilen/ (zugegriffen am 8.3.2020).

Datenschutzbeauftragter-info.de, Die Corona App – Risiken und Nebenwirkungen, Corona - App Risiken, https://www.datenschutzbeauftragter-info.de/die-corona-app-risiken-und-nebenwirkungen/.

Datenschutzgruppe 29, Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, DSGVO angenommen am 3. Oktober 2017.

Datenschutzgruppe 29, WP 29 - Übermittlung personenbezogener Daten an Drittländer, Anwendung von Art. 25 und 26 der Datenschutzrichtlinie der EU (WP 12).

Däubler, Wolfgang/Wedde, Peter/Weichert, Thilo/Sommer, Imke, EU-Datenschutz-Grundverordnung und BDSG-neu, Kompaktkommentar: EU-Datenschutz-Grundverordnung (EU-DSGVO), neues Bundesdatenschutzgesetz (BDSG-neu), weitere datenschutzrechtliche Vorschriften, 2018.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, EU-US Privacy Shield und Datenübermittlungen in die USA, Aufhebung des Safe Harbor Abkommens, Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,

https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/EU-US_PrivacyShield_Daten%C3%BCbermittlungenUSA.html.

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE, Angemessenheitsbeschluss, Glossar, The EU's independent data protection authority, https://edps.europa.eu/data-protection/data-protection/glossary_de.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit, Mecklenburg-Vorpommern, Personalakten und Personalaktendaten, Die folgenden Ausführungen beziehen sich auf den Umgang mit Personalakten und Personalaktendaten in den öffentlichen Stellen des Landes Mecklenburg-Vorpommern. Stand: November 2011 November 2011, https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/persakte.pdf.

Deutsche Gesellschaft für Qualität, Audit im Prozesscontrolling, DGQ-Band 13-41, 1999.

Die eRecht24 GmbH wird vertreten durch: Rechtsanwalt Sören Siebert, Dipl.-Wirtsch.-Inf. Karsten Fernkorn.

Die Landesbeauftragte für Datenschutz - Bremen, Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten, Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Juli 2013, https://www.datenschutz.bremen.de/sixcms/detail.php?gsid=bremen236.c.9283.de.

DIN EN ISO 9001:2008-12 (Deutsche Industrie Norm, Europa Norm, International Organization for Standardization), 12.2008.

Doppler, Klaus/Lauterburg, Christoph, Change Management, Den Unternehmenswandel gestalten, 13. Aufl. 2014.

Drackert, Thoma (Hrsg.), Thoma, ZD 2013, 578, 580 f; Drackert (o. Fußn. 34), S. 280 ff. (zit. als *Bearbeiter* in Drackert).

Drucker, Peter F./Gebauer, Stephan/Simon, Hermann, Was ist Management?, Das Beste aus 50 Jahren, 7. Aufl. 2014.

dsgvo-portal.de, Vgl. https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php, Bußgeld-Datenbank 2020.

DuD, 3/2018, S. 145 1. Datenschutzbeauftragter nach der DSGVO.

DuD, Benedikt Buchner, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter DS-GVO, in Datenschutz Datensich 2016, 155.

DuD, Datenschutz und Datensicherheit, 03/2018, 131 – 202, S. 139 Abs. 1.

DuD, Datenschutz und Datensicherheit, 03/2018, 131 - 202, S. 139 Abs. 3.

DUDEN Onlien, Kohärenz, https://www.duden.de/rechtschreibung/Kohaerenz.

Dudenredaktion, Das Bedeutungswörterbuch, 5. Aufl. 2018.

EDPB = European Data Protection Board.

Eisemann, Hans, Personalbuch 2019, Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht, hrsg. von Jürgen Röller, Wolfdieter Küttner, 26. Aufl., 2019.

Erich-Schmidt-Verlag, Datenschutz-Grundverordnung (DS-GVO), Bundesdatenschutzgesetz (BDSG), Kommentar, 2017.

EU-Data Protection Law (Hrsg.), The risk revolution in EU data protection law, S. 21 f., abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3000382. (zit. als *Bearbeiter* in EU-Data Protection Law).

EuGH C-135/82, Slg 1982, 3799 Rn-10; C-43/77. Slg 1977, 2175 Rn. 22/27; C-157/80, Slg 1981, 1391 Rn.11; C-64/81, Slg 1982, 13 Rn.8, C-34/82, Slg 1983 Rn.9f; C-5/08, Slg 2009, I-06569 Rn.27; C-510/10, ECLI:EU:C:2012:244 Rn.33.

Europäische Union, EMPFEHLUNG DER KOMMISSION vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (Bekannt gegeben unter Aktenzeichen K(2003) 1422) (2003/361/EG), L 124/36, Artikel 2, in Amtsblatt der Europäischen Union.

-*Eurostat*- (Hrsg.), Wichtigste Variablen der Unternehmensdemografie, Online Datencode: TIN00170, letzte Aktualisierung 12.03.2020 Stand 2017.

Faust/Spittka/Wybitul, Milliardenbußgelder nach der DS-GVO? Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz, in Zeitschrift für Datenschutz, S. 105.

Feiler, Lukas/Horn, Bernhard, Umsetzung der DSGVO in der Praxis, Fragen, Antworten, Muster, 2018.

Felix Bieker/Marit Hansen RDV / Recht der Datenverarbeitung Heft 4, 165 f.

Felix Bieker/Marit Hansen/Dr. Michael Friedewald RDV / Recht der Datenverarbeitung Heft 4/2016, 188.

Fitting, Karl/Auffarth, Fritz/Kaiser, Heinrich, Betriebsverfassungsgesetz, 30. Aufl. 2020.

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, Datenschutz-Folgenabschätzung für die Corona-App, Version 1.6 - 29. April 2020, https://www.fiff.de/dsfa-corona.

Franck, Lorenz, Dr PinG - Privacy in Germany Heft 1/2018, 41.

Gabler Wirtschaftslexikon, Revision von Change Management vom 14.02.2018 - 17:31 2018, https://wirtschaftslexikon.gabler.de/definition/change-management-28354/version-251986 (zugegriffen am 14.2.2018).

Gabler Wirtschaftslexikon, Compliance, Definition: Was ist "Compliance", https://wirtschaftslexikon.gabler.de/definition/compliance-27721/version-333143 (zugegriffen am 10.9.2018).

Gabler Wirtschaftslexikon, Cookie, Definition Cookie, Revision von Cookie vom 19.02.2018 06.2020, https://wirtschaftslexikon.gabler.de/definition/cookie-27577/version-251226.

Gabler Wirtschaftslexikon, Definition Risiko 2020, https://wirtschaftslexikon.gabler.de/definition/risiko-44896/version-268200 (zugegriffen am 9.3.2020).

Gabler Wirtschaftslexikon, EBITDA - Earnings before Interest, Taxes, Depreciation and Amortization, Unternehmensbewertung, https://wirtschaftslexikon.gabler.de/definition/earnings-interest-taxes-depreciation-and-amortization-ebitda-35471/version-327317 (zugegriffen am 30.8.2020).

Gabler Wirtschaftslexikon, SWOT Analyse, dt. Abk. für Analysis of strengths, weakness, opportunities and threats, https://wirtschaftslexikon.gabler.de/definition/swot-analyse-52664/version-275782.

Gadatsch, Andreas, Grundkurs Geschäftsprozess-Management, Analyse, Modellierung, Optimierung und Controlling von Prozessen, 9. Aufl. 2020.

Gellert (Hrsg.), EDPL 2016, 481 (zit. als *Bearbeiter* in Gellert).

Gellert (Hrsg.), IRIS 2017 Tagungsband, S. 527 (zit. als *Bearbeiter* in Gellert).

Gellert (Hrsg.), Journal of Internet Law 2015, 3 (zit. als *Bearbeiter* in Gellert).

Gesetzentwurf der Bundesregierung, Drucksache 18/11325, Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes, Drucksache 18/11325, Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU-DSAnpUG-EU).

Gierschmann, Sibylle, Systematischer Praxiskommentar Datenschutzrecht (E-Book), Datenschutz aus Unternehmenssicht, 2014.

Gola, Peter, Handbuch Beschäftigtendatenschutz, Aktuelle Rechtslage und Umsetzungshilfen, 8. Aufl. 2019.

Gola, Peter/Jaspers, Andreas/Müthlein, Thomas/Schwartmann, Rolf, Datenschutz-Grundverordnung im Überblick, Erläuterungen, Schaubilder und Organisationshilfen für die Datenschutzpraxis, 2. Aufl. 2017.

Gola, Peter/Reif, Yvette, Praxisfälle Datenschutzrecht, Juristische Sachverhalte prüfen, bewerten und lösen: 30 Fälle mit Lösungsskizzen und Erläuterungen, 2. Aufl. 2016.

Gola, Peter/Wronka, Georg, Handbuch Arbeitnehmerdatenschutz, Rechtsfragen und Handlungshilfen, 6. Aufl. 2013.

Gruenwald Henderson, Juliana, Kaplan Peter, Office of Public Affairs, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, FTC settlement imposes historic penalty, and significant requirements to boost accountability and transparency, FTC - Federal Trade Commission July 24, 2019, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

Haniel, Erich/Geiger, Martin/Schmutterer, Willi, Gesetz über Ordnungswidrigkeiten, (OWiG); erl. Textausg. mit Vollzugsbestimmungen u. sonstigen einschlägigen Vorschriften unter bes. Berücksichtigung des Straßenverkehrsrechts, 1983.

Hansen, Marit / Walcza, Benjamin RDV / Recht der Datenverarbeitung Heft 2/2019, 53.

Höf-Bausenwein, Heike, Crashkurs Personalarbeit - inkl. Arbeitshilfen online, Vom Arbeitsvertrag bis zum Zeugnis, 3. Aufl. 2018.

https://www.it-daily.net/it-sicherheit/datenschutz/16901-die-eu-dsgvo-kommt-haben-sie-einen- plan-was-zu-tun-ist.

In Anlehnung an den Fragebogen des Bayerischen Landesamt für Datensicherheit, In Anlehnung an den Fragebogen des Bayerischen Landesamt für Datenschutzaufsicht, (www.lda.bayern.de), Fragebogen, www.lda.bayern.de.

In Anlehnung an Grafik Gap-Analyse, https://wirtschaftslexikon.gabler.de/definition/gap-analyse-34738.

Informatik-verstehen.de, Der Quellcode, auch bekannt als Quelltext oder Source Code, ist eine Textdatei im Standard-ASCI-Format, die alle Befehle und Anweisungen eines mit einer höheren Programmiersprache erstellten Programms enthält, https://www.informatik-verstehen.de/lexikon/quellcode/.

Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen, 06.2017.

Ingelheim, Alexander, Fircks, Isabelle, Fünkner, Dominik, VORLAGE DATENSCHUTZINFORMATIONEN FÜR BEWERBER,

https://www.datenschutzexperte.de/fileadmin/user_upload/PDFs/Datenschutzinformation-Muster-Bewerber.pdf.

International Organization for Standardization, Qualitätsmanagement ISO 9001, Was ist ein Prozessaudit?, https://www.qualitaetsmanagement.me/iso_9001_audit/prozessaudit/ (zugegriffen am 18032020).

International Organization for Standardization, Qualitätsmanagement ISO 9001, Was ist ein Produktaudit?, https://www.qualitaetsmanagement.me/iso_9001_audit/produktaudit/ (zugegriffen am 18032020).

International Organization for Standardization, Qualitätsmanagementsysteme - Grundlagen und Begriffe (ISO 9000:2005), DIN EN ISO 9000:2005, 12.2005.

John P. Kotter, Wye Transformation Efforts Fail, in Havard Business Manager März / April 1995.

Jung, Alexander, Datenschutz-(Compliance-)Management-Systeme- Nachweis-und Rechenschaftspflichten nach der DSGVO., Praktische Ansätze für die Erfüllung ordnungsgemäßer Datenverarbeitung, in ZD - Zeitschrift für Datenschutz 2018, 208.

Jung, Niklas, Abolition of the Safe Harbour Agreement: Legal situation and alternatives 2016, http://hdl.handle.net/10419/148370.

Kamiske, Gerd F./Brauer, Jörg-Peter, Qualitätsmanagement von A - Z, Wichtige Begriffe des Qualitätsmanagements und ihre Bedeutung, 2016.

Kampffmeyer, Ulrich, http://www.project-consult.de/files/S 113EIA_H_2013. pdf, S. 17 ff., Revisionssicherheit von Archivierungssystemen, Eingabekontrolle, Plausibilitätskontrolle, Transaktionskontrolle 2013.

Karsten U. Bartels LL.M., Merlin Backer LL.M., Die Berücksichtigung des Stands der Technik in der DSGVO, Neue Anforderungen an die IT-Sicherheit im Datenschutz, in Datenschutz Datensich, 214 f.

Klinger & Reicher Rechtstext Verlag, EU-Datenschutz-Grundverordnung DSGVO, 28.07.2019.

Konferenz der unabhängigen Datenschutzaufsichtsbehörden, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien März 2019.

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz, Videoüberwachung nach der Datenschutz-Grundverordnung, Kurzpapier Nr. 15 17.12.2018, 1.

Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren, 11.2015.

Körffer, Barbara/Klug, Christoph/Gola, Peter/Schomerus, Rudolf, Bundesdatenschutzgesetz, BDSG; Kommentar a.F., 10. Aufl. 2010.

Kotter, John P., Leading change, Wie Sie Ihr Unternehmen in acht Schritten erfolgreich verändern, 2015.

Kühling / Buchner/Bergt Art. 82 Rn. 60; Lauel/Nink/Kremer, § 11 Rn. 14; Sydow/Kreße Art. 82 Rn. 23, Rechtsbehelfe, Haftung und Sanktionen, hrsg. von Sydow/Kreße Kühling /Buchner/Bergt (zit. als *Bearbeiter* in Kühling / Buchner / Bergt Art. 82 Rn. 60; Lauel / Nink / Kremer, § 11 Rn. 14; Sydow / Kreße Art. 82 Rn. 23).

Kühling, Jürgen/Klar, Manuel/Sackmann, Florian, Datenschutzrecht, 4. Aufl. 2018.

Kutscha, Martin, Das „Computer-Grundrecht“ — eine Erfolgsgeschichte?, zum Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 - - 1 BvR 595/07 -, in Datenschutz Datensich 2012, 391.

Lachenmann, Matthias, Datenübermittlung im Konzern, Dissertation, 2016.

Lachenmann, Matthias, Neue Anforderungen an die Videoüberwachung, Videoüberwachung nach BDSG-neu, in ZD - Zeitschrift für Datenschutz, 407.

Landesbeauftragter Für Datenschutz und Informationsfreiheit, Baden-Württemberg, Beschäftigtendatenschutz: Zwischen wirtschaftlicher und persönlicher Abhängigkeit und informationeller Selbstbestimmung, Ratgeber Beschäftigten Datenschutz März 2018, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/Ratgeber-ANDS-2.-Auflage.pdf.

Laue, Philip/Kremer, Sascha, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl. 2019.

Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, § 11, Rn. 15, geht von einem solchen in jedem Fall bei Art. 6, 9, 10, 15-22, 25 und 32 EU-DSGVO aus; „weitestgehend“ alle Anforderungen der DSGVO als Schutzgesetz ansehend Wybitul/Haß/Albrecht, NJW 2018, 113, 113; a.A. weiter wohl Gola/Piltz, in Gola, DSGVO, Art. 82, Rn. 26, gemäß Art. 1 Abs. 1 DSGVO sei jeder Norm der DSGVO als Schutzgesetz i.S.v. §823 Abs.2 BGB einzustufen., Datenschutzrecht (zit. als *Bearbeiter* in Datenschutzrecht in der betrieblichen Praxis).

Lauer, Thomas, Change Management, Grundlagen und Erfolgsfaktoren, 2. Aufl. 2014.

Little, David B./Chapa, David A., Implementing backup and recovery, The readiness guide for the enterprise (VERITAS series), 2003.

Loomans, Dirk/Matz, Manuela/Wiedemann, Michael, Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, Ein risikobasierter Ansatz für alle Unternehmensgrößen, 2014.

Marshall, Kevin, Rechtsverträgliche Gestaltung, in Datenschutz und Datensicherheit - DuD, 183.

Marzi, Christian/Pallwein-Prettner, Angelika, Datenschutzrecht, Auf Basis der EU DS-GVO, 2018.

Meier, Markus, Projektmanagement, Situationsanalyse, Zielbestimmung, Projektcontrolling, Controllingwerkzeuge, Motivation, Teammanagement, 2007.

Moos, Flemming/Schefzig, Jens/Arning, Marian, Die neue Datenschutz-Grundverordnung, Mit Bundesdatenschutzgesetz 2018, in De Gruyter Praxishandbuch.

Nohr, Holger, Big Data im Lichte der EU-Datenschutz-Grundverordnung - JurPC-Web-Dok. 0111/2017, Big Data im Lichte der EU-Datenschutz-Grundverordnung, 0111. Aufl., hrsg. von Holger Nohr, 2017 (zit. als *Bearbeiter* in Big Data im Lichte der EU-Datenschutz-Grundverordnung).

Ordnungswidrigkeiten, in RDV - Recht auf Datenverarbeitung 2017.

ORF - österreichischer Rundfunk, Drohnen zur Überwachung der Ausgangssperre in Spanien, Drohnen kontrollieren Ausgangssperre, Der ORF, Würzburggasse 30, 1136 Wien 17. März 2020, 13.28 Uhr, https://orf.at/stories/3158224/ (zugegriffen am 5.4.2020).

Otto, Hansjörg, BetrVG 1972 § 87: Anmerkung zu BAG 2 AZR 51/02 (AP: BetrVG 1972 § 87 Überwachung, Nr. 36), in Nachschlagewerk des Bundesarbeitsgerichts : AP, arbeitsrechtliche Praxis ; die Rechtsprechung des Bundesarbeitsgerichts und die arbeitsrechtlich bedeutsamen Entscheidungen anderer Gerichte mit erläuternden Hinweisen ; Wiedergabe der Leitsätze und Fundstellennachweise ; Kurzausgabe 2005, 87.

Pachinger, Michael M./Beham, Georg, Datenschutz-Audit, Recht - Organisation - Prozess - IT: der Praxisleitfaden zur Datenschutz-Grundverordnung, 2017.

Palandt, Otto/Bassenge, Peter, Bürgerliches Gesetzbuch, Mit Nebengesetzen, insbesondere mit Einführungsgesetz (Auszug) einschließlich Rom-I-, Rom-II- und Rom-III-Verordnungen sowie Haager Unterhaltsprotokoll und EU-Erbrechtsverordnung, Allgemeines Gleichbehandlungsgesetz (Auszug), Wohn- und Betreuungsvertragsgesetz, BGB-

Informationspflichten-Verordnung, Unterlassungsklagengesetz, Produkthaftungsgesetz, Erbbaurechtsgesetz, Wohnungseigentumsgesetz, Versorgungsausgleichsgesetz, Lebenspartnerschaftsgesetz, Gewaltschutzgesetz, 74. Aufl. 2015.

Pech, Anton/Jens, Klaus/Warmuth, Günter/Zeininger, Johannes, Parkhäuser - Garagen, Grundlagen, Planung, Betrieb, 2009.

Pillkahn, Ulf, Trends und Szenarien als Werkzeuge zur Strategieentwicklung, Wie Sie die unternehmerische und gesellschaftliche Zukunft planen und gestalten, 2007.

Piltz, Carlo, BDSG, Praxiskommentar für die Wirtschaft, 2018.

Plate, Markus, Grundlagen der Kommunikation, Gespräche effektiv gestalten, 2. Aufl. 2015.

Pressestelle, Datenschutz und die Informationsfreiheit Baden-Württemberg, DATENSCHUTZVERLETZUNGEN BEREITEN ZUNEHMEND SORGE!, Die am häufigsten gemeldeten Datenschutzverletzungen, Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/07/PM-Datenschutzverletzungen-bereiten-zunehmend-Sorge-30.07.2019.pdf.

Promotorengruppe Kommunikation der Forschungsunion Wirtschaft - Wissenschaft, Im Fokus: Das Zukunftsprojekt Industrie 4.0 - Handlungsempfehlungen zur Umsetzung, März 2012.

Quiring-Kock, DuD, Datenschutz und Datensicherheit 2012, 832.

RA Jaspers, Andreas /RAin Reif, Yvette, LL.M. RDV / Recht der Datenverarbeitung Heft 2/April 2016, 61.

RDV / Recht der Datenverarbeitung 2000, 95f.

RDV Recht auf Datenverarbeitung, Bußgeld im digitalen Zeitalter – was bringt die DS-GVO, 02. Aufl., 2017 (zit. als *Bearbeiter* in Recht auf Datenverarbeitung).

Rechtssache C-362/14, SCHLUSSANTRÄGE DES GENERALANWALTS YVES BOT vom 23. September 2015(1) Rechtssache C-362/14 Maximillian Schrems gegen Data Protection Commissioner.

Reimann, Grit/e.V., DIN., Betrieblicher Datenschutz Schritt für Schritt - gemäß EU-Datenschutz-Grundverordnung, Lösungen zur praktischen Umsetzung Textbeispiele, Musterformulare, Checklisten, 2. Aufl. 2018.

RICHTLINIE (EU) 2016/ 679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES - vom 27. April 2016, Erwägungsgründe - VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien

Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Erwägungsgründe Datenschutz-Grundverordnung, in Amtsblatt der Europäischen Union 04.05.2016.

Rimscha, Markus von, Datenschutz - Konzepte, Algorithmen und Anwendung, Werkzeuge zum Datenschutz im Alltag, 2018.

Rolfs, Christian/Witschen, Stefan, Bürgerliches Gesetzbuch 2002, Anmerkung zu BAG 9 AZR 271/06 (EZA: BGB 2002, § 611 Persönlichkeitsrecht Nr. 4), in Entscheidungssammlung zum Arbeitsrecht 2007, 11.

Romeike, Frank, Risikomanagement, 2018.

Roßnagel / Geminn / Johannes, Datenschutz-Folgenabschätzung im Zuge der Gesetzgebung, Das Verfahren nach Art. 35 Abs. 10 DS-GVO, in ZD - Zeitschrift für Datenschutz, 435.

Roßnagel, Alexander, Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, Neue Aufgaben und Befugnisse der Aufsichtsbehörden, 2017.

Rost, Maria Christina, Datenschutzsanktionen: scharfes Schwert oder Papiertiger?, Datenschutz Datensich (Datenschutz und Datensicherheit - DuD), in Datenschutz Datensich 2019, 488.

Rüpke, Giselher/Lewinski, Kai/Eckhardt, Jens, Datenschutzrecht, Grundlagen und europarechtliche Neugestaltung, 2018.

Sachs, Andreas/Kranig, Thomas/Gierschmann, Markus, Datenschutz-Compliance nach der DS-GVO, Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden, 2017.

Schantz, Peter/Wolff, Heinrich Amadeus, Das neue Datenschutzrecht, Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, 2017.

Schmelzer, Hermann J./Sesselmann, Wolfgang, Geschäftsprozessmanagement in der Praxis, Kunden zufriedenstellen, Produktivität steigern, Wert erhöhen; [das Standardwerk, 7. Aufl. 2010.

Schmidbauer, Klaus/Jorzik, Oliver, Wirksame Kommunikation – mit Konzept, Ein Handbuch für Praxis und Studium, 2017.

Schneider, Jochen, Datenschutz, Nach der EU-Datenschutz-Grundverordnung, 2. Aufl. 2019.

Schröder, Markus, Der risikobasierte Ansatz in der DSGVO, Risiko oder Chance für den Datenschutz, in ZD - Zeitschrift für Datenschutz, 503.

Schwartmann, Rolf/Keber, Tobias O./Mühlenbeck, Robin, Social Media, Soziale Netzwerke und Homepages sicher gestalten und nutzen, 2. Aufl. 2018.

Simon, Walter, Managementkonzepte von A bis Z, Managementtheorien, Führungsstrategien, Führungstools, 2009.

Spindler, Gerald/Schmitz, Peter/Liesching, Marc, Telemediengesetz mit Netzwerkdurchsetzungsgesetz; Kommentar, 2. Aufl. 2018.

Springer Gabler Verlag (Hrsg.), Betriebsvereinbarung, Was ist Betriebsvereinbarung?, Gabler Wirtschaftslexikon, https://wirtschaftslexikon.gabler.de/definition/betriebsvereinbarung-28363/version-251995.

Springer Gabler Verlag (Hrsg.), http://wirtschaftslexikon.gabler.de/Definition/konzern.html, Definition Konzern, Gabler Wirtschaftslexikon.

Springer Gabler Verlag (Hrsg.), Konfliktmanagement, Feststellung, Steuerung und Regelung von Konflikten durch spezifische Handhabungsformen, etwa Verhandlung, Vermittlung, Schlichtung einschließlich Zwangsschlichtung., https://wirtschaftslexikon.gabler.de/definition/konfliktmanagement-41409/version-264774.

Springer Gabler Verlag (Hrsg.), Personalbedarfsermittlung, Gabler Wirtschaftslexikon, https://wirtschaftslexikon.gabler.de/definition/personalbedarfsermittlung-46363/version-269645.

Springer Gabler Verlag (Hrsg.), Personalentwicklung, Gabler Wirtschaftslexikon, https://wirtschaftslexikon.gabler.de/definition/personalentwicklung-52604/version-330100.

Springer Gabler Verlag (Hrsg.), Personalfreisetzung, Gabler Wirtschaftslexikon, https://wirtschaftslexikon.gabler.de/definition/personalfreisetzung-43403/version-266733.

Srdjan Govedarica, ARD-Studio Wien von, Österreich überwacht Handydaten, Coronavirus (Covid 19) 18.03.2020, 16:25 Uhr, https://www.tagesschau.de/investigativ/handyueberwachung-oesterreich-101.html.

Statista GmbH, Prognose zum weltweit generierten Datenvolumen 2025,, https://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/#professional.

Steffen, Nils/DuD, 3/2018, S.145 Nr. 2. Zivilrechtliche Haftung von Datenschutzbeauftragten für Bußgelder, DuD, 3/2018, S.145 Nr. 2. Zivilrechtliche Haftung von Datenschutzbeauftragten für Bußgelder, Datenschutz Grundverordnung, in Datenschutz und Datensicherheit 2018, 145.

The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, CNIL. Commission Nationale de l'Informatique et des Libertés 21. January 2019, https://www.cnil.fr/en/node/287.

Umweltmanagementsysteme - Anforderungen mit Anleitung zur Anwendung (ISO 14001:2015).

VFR Verlag für Rechtsjournalismus GmbH, Muster Datenschutzerklärung, https://www.datenschutz.org/datenschutzerklaerung-muster.pdf.

VFR Verlag für Rechtsjournalismus GmbH, Wer darf die Personalakte laut Datenschutz einsehen?, https://www.datenschutz.org/personalakte/.

Voigt, Paul/dem Bussche, Axel von, EU-Datenschutz-Grundverordnung (DSGVO), Praktikerhandbuch, 2018.

Voßhoff, Andrea, Hermerschmidt, Sven PinG - Privacy in Germany Heft 02/2016, 56.

Wagner, Richard, Strategie und Managementwerkzeuge, Marktanalyse, Geschäftsfeldplanung, Strategieentwicklung, Unternehmensführung, Marketing, 2007.

Walter, Axel, Datenschutz im Betrieb - DS-GVO in der Personalarbeit, 2018.

Warren, Samuel D., Brandeis, Louis D., Harvard Law Review Vol. IV. December 15, 1890. No. 5. The Right to Privacy, 23. Juli 2015.

Wiebke Reuter LL.M., Umgang mit sensiblen Daten bei allgemeiner Videoüberwachung, Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten, in ZD - Zeitschrift für Datenschutz, 564.

Winterstein/Ceyssens/Wessely, in: Groeben/Schwarze/Hatje, AEUV, 7. Auflage, nach Art, 101, Rn. 46 ff. und vor allem Rn. 86 ff., Art. 83 Abs. 2 lit. f, hrsg. von in Groeben/Schwarze/Hatje Winterstein/Ceyssens/Wessely (zit. als *Bearbeiter* in Art. 83 Abs. 2 lit. f).

Wirtschaftsanalyse24.com, Gap-Analyse 2018, http://www.wirtschaftslexikon24.com/d/gap-analyse-lueckenanalyse/gap-analyse-lueckenanalyse.htm (zugegriffen am 7.3.2020).

Wirtschafts-Lexikon, Das Wissen der Betriebswirtschaftslehre, 2006.

Wirtschafts-Lexikon, Das Wissen der Betriebswirtschaftslehre, 2006.

Witt, Bernhard C., Datenschutz kompakt und verständlich, Eine praxisorientierte Einführung, 2008.

Wybitul, RA, Tim, / Draf, Dr. Oliver, LL.M., Wybitul/Draf · Projektplanung und Umsetzung der EU-Datenschutz-Grundverordnung im Unternehmen, Prozessschritte zur Einführung der DSGVO im Unternehmen, in Betriebsbs-Berater 2016.

Wybitul, Tim, EU-Datenschutz-Grundverordnung im Unternehmen, Praxisleitfaden, 2016.

III. Fragebogen Einführung / Auswirkungen Datenschutz-Grundverordnung

Vertraulich? Ja / Nein

Name des Unternehmens: _____

Sitz des Unternehmens: _____

Anzahl MitarbeiterInnen:

- Deutschland _____
- Europa- / Weltweit _____

Name des Ansprechpartners: _____

Name des Datenschutzbeauftragten: _____

Name des für die Verarbeitung Verantwortlichen: _____

Art der Befragung:

- Telefonisch ☐
- Persönlich ☐
- Per Mail ☐
- Im Chat ☐
- Per Videokonferenz ☐

Konzernstrukturen vorhanden? Ja / Nein

Kurze Beschreibung:

_____

_____

Wann haben sie mit der Einführung begonnen?

- Datum: _____

Wurde die Einführung von externen Spezialisten begleitet? Ja / Nein

- Welcher Art: _____

Wurde ein interner oder externer Datenschutzbeauftragter „bestellt“?

- Externe Variante ☐
- Interne Variante ☐

Existier(t)en ein oder mehrere Konzernbeauftragte(r) für den Datenschutz? Ja / Nein

Wurden die Mitarbeiterinnen und Mitarbeiter im Vorfeld geschult? Ja / Nein

- In-house Schulungen ☐
- Externe Schulungen ☐
- Wiederkehrende Schulungen? Ja / Nein

Wurden regelmäßige Termine angesetzt (Jour Fix)? Ja / Nein

Wurden zur Einführung bestehende Strukturen angepasst? Ja / Nein

- Wenn Ja, welche Strukturen wurden angepasst?

Beschreibung der Änderungen:
_____
_____
_____

Wurde zusätzliches Personal eingestellt? Ja / Nein

Beschreibung:
_____
_____

Wurden im Vorfeld und im Anschluss Budgetierungen vorgenommen? Ja / Nein

Beschreibung:
_____
_____
_____

Wurden technische Maßnahmen umgesetzt? Ja / Nein

Datenschutzerklärung (Webseite) Ja / Nein

Privacy by Design Ja / Nein

Privacy By Default Ja / Nein

Beschreibung:

Sind nach Einführung der DS-GVO Beschwerden eingegangen? Ja / Nein

- Wenn Ja, welcher Art waren diese?

Beschreibung:

Konnten die vorgegebenen Fristen eingehalten werden? Ja / Nein

Anmerkungen:

Hat die Einführung der Datenschutz-Grundverordnung zu den anfänglich befürchteten Umsatzeinbußen geführt? Ja / Nein

Wenn Ja, welcher Art waren diese?

Beschreibung:

Werden biometrische Daten verarbeitet? Ja / Nein

Wenn Ja, welcher Art:

Beschreibung:

Allgemeine Erfahrungen

Beschreibung:

Auswirkungen auf den betrieblichen Alltag

Beschreibung:

Beschreibung:

Besteht die Möglichkeit bei zusätzlichen Fragen den Datenschutzbeauftragten / Verantwortlichen zu kontaktieren? Ja / Nein

Wenn Ja, auf welche Weise:

- Telefon: _____
- Mobil: _____
- E-Mail: _____
- Persönlich: _____
- Fax _____
- Chat _____

Einwilligung / Erklärung

Ich / wir [Name des Verantwortlichen _____] erkläre(n) mich / uns mit der Nutzung / Veröffentlichung der Durchgeführten Befragung grundsätzlich einverstanden.

Ja / Nein

Einschränkungen? _____

Es ist dem Interviewer explizit gestattet, alle Namen, Fakten und Daten des Interviewpartners die auf Grundlage des Interviews entstanden sind, zu verwenden und zu veröffentlichen.

Ja / Nein

Einschränkungen? _____

Sie wurden darüber informiert, dass die Speicherung, Nutzung und Verarbeitung personenbezogener Daten nicht gestattet ist. Eine Verwendung nur, wenn sie ihr Einverständnis in Form einer freiwilligen Einwilligung geben. Ja / Nein

Die Einwilligung hat dabei grundsätzlich eindeutig und erkennbar zu sein. Weiterhin muss der Verwendungszweck eindeutig erkennbar sein. Darüber hinaus muss aus der Erklärung das Recht des Betroffenen, Löschung, Auskunft und Widerspruch hervorgehen. Sie erklären hiermit unmissverständlich die Einwilligung zur Vorliegenden Befragung, im Wissen darüber, dass die erklärten Punkte personenbezogene Daten enthalten könnten. . Ja / Nein

Ihre Einwilligung können Sie jederzeit gegenüber Murad Erserbetci widerrufen, mit der Folge, dass die Verarbeitung Ihrer personenbezogenen Daten, nach Maßgabe Ihrer Widerrufserklärung, durch diesen für die Zukunft unzulässig wird. Dies berührt die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung jedoch nicht.

Rechtsgrundlage

Murad Erserbetci (nachfolgend M.E) verarbeitet die von Ihnen erhobenen personenbezogene Daten auf Basis Ihrer Einwilligung gemäß Art. 6 Abs. 1 S. 1 lit. a DS-GVO. Sofern besondere Kategorien personenbezogener Daten betroffen sind, verarbeitet M.E die von Ihnen erhobenen personenbezogenen Daten auf Basis Ihrer Einwilligung gemäß Art. 9 Abs. 2 lit. a DS-GVO.

Empfänger oder Kategorien von Empfängern / Drittstaatenübermittlung

An folgende Empfänger oder Kategorien von Empfängern werden Ihre personenbezogenen Daten durch M.E übermittelt oder können übermittelt werden:

- Prof. Dr. Dr. Thomas Gergen (Business Science Institute, Betreuer)
- Yasemin Ozuag (Business Science Institute, DBA Program Coordinator)
- Prof. Dr. Anne Bartel-Radic (Business Science Institute, Koordinatorin deutsches DBA – Programm)
- Prof. Dr. André Reuter (Business Science Institute, Vorstands des Europäischen Instituts für Wissens- und Werte-Management (EIKV).

Dauer, für die die personenbezogenen Daten gespeichert werden / Kriterien für die Festlegung der Dauer

- Bis zur Beendigung des Dissertationsverfahrens, darüber hinaus maximal 2 Jahre

Ihre Rechte

Im Rahmen der gesetzlichen Vorgaben haben Sie gegenüber **M.E** grundsätzlich Anspruch auf:

- Bestätigung, ob Sie betreffende personenbezogenen Daten durch **M.E** verarbeitet werden,
- Auskunft über diese Daten und die Umstände der Verarbeitung,
- Berichtigung, soweit diese Daten unrichtig sind,
- Löschung, soweit für die Verarbeitung keine Rechtfertigung und keine Pflicht zur Aufbewahrung (mehr) besteht,
- Einschränkung der Verarbeitung in besonderen gesetzlich bestimmten Fällen und
- Übermittlung Ihrer personenbezogenen Daten – soweit Sie diese bereitgestellt haben – an Sie oder einen Dritten in einem strukturierten, gängigen und maschinenlesbaren Format.

Darüber hinaus haben Sie das Recht, Ihre Einwilligung jederzeit gegenüber **M.E** zu widerrufen, mit der Folge, dass die Verarbeitung Ihrer personenbezogenen Daten, nach Maßgabe Ihrer Widerrufserklärung, durch diesen für die Zukunft unzulässig wird. Dies berührt die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung jedoch nicht.

Interviewer	Interviewpartner(in)
Ort, Datum, Name	Ort, Datum, Name
Unterschrift	Unterschrift

IV. Formular
Technisch Organisatorische Maßnahme (TOM)

Nachfolgendes Formular umfasst, nicht abschließend, mehrere Bereiche, um bei direkter Nutzung einen größtmöglichen Gestaltungsraum nutzen zu können.

§ 1 Allgemeine Informationen

a) Geltungsbereich

Dieses Dokument ist Teil der Datenschutzdokumentation des Datenschutzmanagementsystems der [Firma]. Das vorliegende Dokument ist ein Dokument der Ebene [Bezeichnung] gemäß den Kennzeichnungs- und Klassifizierungsrichtlinien der [Firma]. Aufgrund der Vereinfachung der Darstellung wird im Folgenden für alle Rollen-, Stellen-, und Funktionsbezeichnungen die männliche Form, stellvertretend für die weibliche und männliche Schreibweise, verwendet.

Dieses Dokument gilt für die informationsverarbeitenden Systeme und Netzwerke, Dokumente und Informationen der (gesamten) [Firma], mit denen personenbezogene Daten erhoben, verarbeitet und genutzt (gespeichert) werden.

Diese Version des Dokumentes ersetzt alle früheren Versionen und Ausgaben. Sollten vertragliche oder gesetzliche Festlegungen dieses Dokument oder Teile hiervon berühren, haben diese in jedem Fall Vorrang. Die Aktualisierung und Weiterentwicklung dieses Dokumentes obliegen dem Datenschutzbeauftragten der [Firma]. Der Ausdruck dieses Dokumentes mit dem Vermerk „Original“ stellt eine gelenkte Kopie dar und unterliegt dem Änderungsdienst.

Die nachfolgende Liste dient nur der erläuternden Darstellung gesetzlicher Anforderungen in Bezug auf den Datenschutz. Die Rechte und Pflichten der Parteien ergeben sich allein aus den vertraglichen Vereinbarungen und den gesetzlichen Bestimmungen zum Datenschutz. Insofern können aus dieser Liste keine Ansprüche abgeleitet werden. Technische Änderungen und/oder Änderungen in der Organisation, die keinen Einfluss auf die Erfüllung der gesetzlichen Anforderungen der DS-GVO in der jeweils aktuellen Fassung haben, bedürfen keiner gesonderten Information gegenüber dem Vertragspartner. Die angegebenen Punkte können je nach Vertrag / Leistungsschein

variieren. Vor einer Nutzung ist die Rechtmäßigkeit des Inhaltes zu überprüfen und entsprechend anzupassen.

b) Beschreibung des Aufbaus der Prüfliste

Die Fragen der Prüfliste sind mit folgenden Punkten überschrieben:

Nr.	laufende Nummerierung der jeweiligen Prüfabschnitte
Frage	datenschutzrelevante Fragestellung
Antwort	Beantwortung auf Basis aktueller Prozesse und Verfahren im Unternehmen Ankreuzantworten nach Stand der Technik
Anmerkung	Kommentar- oder Anmerkungsfeld für erklärende Hinweise zur Art der Umsetzung oder Notizen für den Datenschutzbeauftragten

c) geprüftes Rechenzentrum

genaue Anschrift des geprüften Rechenzentrums:

PLZ und Ort:	
Straße und Hausnummer:	
Etage, Raumnummer:	
Systemstandort: Käfignummer Schranknummer (Rack) Höheneinheit	
Bezeichnung	

d) Unterauftragnehmer

Genaue Firmierung:	
Datenschutzbeauftragter:	
PLZ und Ort:	
Straße und Hausnummer:	
Etage, Raumnummer:	

e) Prüfung

	Prüfer	begleitet/abgenommen durch Verantwortlichen des Kunden:
Vor-/Nachname:		
Rolle:		
Unternehmen:		
beauftragt durch:		
bestätigt am:	Datum und Unterschriften der Datenschutzbeauftragten	

f) gültige Zertifizierungen

Zertifizierungen hier genau aufführen:	gültig bis:

g) geplante Zertifizierungen

§ 2 Zutrittskontrolle

Nr.	*Frage*	*Antwort*	*Anmerkungen*
2.1	Wer ist für die Zutrittskontrolle beim Auftragnehmer verantwortlich?	□ RZ-Verantwortlicher □ Abteilung bei Auftragnehmer □ Sonstige: _____ □ Regelung vorhanden: ja/nein	
2.2	Wer legt die zu sichernden Objekte und Bereiche beim Auftragnehmer fest?	□ IS-/IT-Sicherheitsbeauftragte(r) □ RZ-Verantwortlicher □ Andere: _____ □ Regelung vorhanden: ja/nein	
2.3	Werden die Zutrittsrechte dokumentiert?	ja/nein Dokument: Datum/Version:	
2.4	Gibt es ein dokumentiertes Verfahren für die Vergabe/Entzug von Zutrittsrechten?	ja/nein	
2.5	Werden Anwesenheitsaufzeichnungen im Sicherheitsbereich geführt?	ja/nein	
2.6	Welche Personen, die nicht beim Auftragnehmer angestellt sind, verfügen über Zutrittsberechtigungen?	□ keine □ Liste vorhanden □ Datum der Liste:	
2.7	Durch welche weiteren organisatorische/technische Maßnahmen wird die Zutrittskontrolle unterstützt?	□ Alarmanlage □ Videoüberwachung	

Nr.	*Frage*	*Antwort*	*Anmerkungen*
		□ Gebäudebewachung (Wachschutz) □ Vereinzelungsschleuse □ Andere:	
2.8	Sind die Eingangstüren und Nebentüren gesichert, so dass ein Schutz vor unbemerktem Betreten/Verlassen der Gebäude besteht?	ja/nein	
2.9	Werden Externe in den Gebäuden beaufsichtigt?	ja/nein	
2.10	Werden Besucher zum Besuchten begleitet bzw. von ihm abgeholt?	ja/nein	
2.11	Werden Besucher erfasst?	□ Besucherbuch/-liste □ elektronisches Ausweissystem □ Andere:	
2.12	Werden Fenster und nach außen gehende Türen verschlossen, wenn die Räume, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet, nicht besetzt sind?	ja/nein	
2.13	Sind einstiegsgefährdete Fenster und Türen in Gebäuden, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet, gegen Einbruch abgesichert?	ja/nein	
2.14	Welche Personen dürfen die Serverräume und/oder das Rechenzentrum betreten?	Serverräume: □ Haustechnik □ Infrastrukturteam □ IT-Systemtechniker □ Geschäftsführung □ Reinigungspersonal □ Sonstige: _____ Rechenzentrum: □ Haustechnik □ Infrastrukturteam □ IT-Systemtechniker □ Geschäftsführung □ Reinigungspersonal □ Sonstige: _____	
2.15	Sind die Serverräume bzw. das Rechenzentrum vor dem Zutritt unberechtigter Personen – insbesondere auch außerhalb der Geschäftszeiten – geschützt?	Serverräume: ja/nein Rechenzentrum: ja/nein	
2.16	Durch welche Maßnahmen wird der Zutritt zu DV-, TK-Systemen für Unbefugte verwehrt?	□ Einteilung in Sicherheitszonen/Sperrbereiche □ Closed Shop Betrieb □ automatische Zutrittskontrolle □ Berechtigungsausweis	

Nr.	*Frage*	*Antwort*	*Anmerkungen*
		□ Schlüsselregelung □ Personenkontrolle durch Pförtner □ Sonstiges:	
2.17	Welche störenden Einflüsse existieren beim Auftragnehmer in Räumen bzw. Gebäuden, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet?	□ Hitze, Kälte, Feuchtigkeit □ HF-Strahlung und elektromagnetische Kraftfelder □ Bahnanlagen/Oberleitungen □ Stromausfall oder Stromschwankungen während des laufenden Betriebs □ Sonstiges:	
2.18	Werden schädigende Umgebungseinflüsse in Räumen bzw. Gebäuden, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet, bei der Installation und der Benutzung von IT-Komponenten beachtet?	ja/nein	

§ 3 Zugangskontrolle

Nr.	*Frage*	*Antwort*	*Anmerkungen*
3.1	Welche Maßnahmen schützen IT-Systeme vor unbefugter Nutzung?	□ Passwortvergabe □ Protokollierung der Passwortnutzung □ Sonstige: _____	
3.2	Existieren für Mitarbeiter(innen) des Auftragnehmers, die Daten des Auftraggebers verarbeiten und/oder speichern bzw. Systeme betreuen, Hinweise über den Umgang mit administrativen Passwörtern?	ja/nein Dokument: _____ Version/Datum: _____	
3.3	Verfügt jeder Berechtigte über ein eigenes, nur ihm bekanntes Passwort?	ja/nein	
3.4	Gibt es Gruppenpasswörter, die von mehreren Nutzern eingesetzt werden?	ja/nein	
3.5	In welchen Bereichen und zu welchem Zweck werden Gruppenpasswörter eingesetzt?	Bereich / Zweck /	
3.6	Wird dokumentiert, wann welcher Mitarbeiter das Gruppenpasswort benutzt hat?	ja/nein	
3.7	Gibt es eine Passwortrichtlinie, die die Struktur eines Passwortes, sowie die Änderungsintervalle und Nutzung beschreibt?	ja/nein Dokument: _____ Version/Datum: _____	
3.8	Sind Mitarbeiter des Auftragnehmers, die Daten des Auftraggebers verarbeiten/speichern aufgefordert komplexe Passwörter einzusetzen?	ja/nein	

Nr.	*Frage*	*Antwort*	*Anmerkungen*
3.9	Wann werden Passwörter für IT-Systeme/Nutzer gewechselt?	IT-Systeme: nie/alle ___ Tage Nutzer: nie/alle ___ Tage □ Regelung vorhanden: ja/nein	
3.10	Welche Mindestlänge haben diese Passwörter?	Anzahl der Stellen: □ Regelung vorhanden: ja/nein	
3.11	Werden Passwörter für IT-Systeme/Nutzer nur verschlüsselt abgespeichert oder übertragen?	IT-Systeme: ja/nein Nutzer: ja/nein	
3.12	Gibt es für IT-Systeme/Nutzer eine Passwort-Historie, um zu vermeiden, dass alte Passwörter weiterverwendet werden?	IT-Systeme: ja/nein Nutzer: ja/nein	
3.13	Werden Administrationspasswörter für IT-Systeme gesichert aufbewahrt?	ja/nein	
3.14	Werden Schlüssel für Kryptographie-Verfahren gesichert aufbewahrt?	ja/nein	
3.15	Wie oft kann sich ein Benutzer an IT-Systemen vergeblich anmelden, bis der Zugriff automatisch gesperrt wird?	□ unbegrenzt □ nach __ Anmeldeversuchen	
3.16	Wie erfolgt im Falle der Sperrung eines Administrationszugangs die Entsperrung vorgenommen?	□ undokumentiertes Verfahren □ Service Desk	
3.17	Sind die Passwörter der Mitarbeiter(innen) für IT-Systeme auch dem Administrator und/oder dem Management bekannt?	ja/nein	
3.18	Werden über alle Aktivitäten auf DV-Anlagen automatisch Protokolle erstellt?	ja/nein	
3.19	Von wem werden diese Protokolle hinsichtlich etwaiger Unregelmäßigkeiten ausgewertet und in welchen zeitlichen Abständen erfolgt dies?	Auswertung: □ manuell □ automatisiert Zeitintervalle: (täglich / wöchentlich / monatlich) □ nie	
3.20	Wie werden IT-Systeme gegen unbefugte Nutzung abgesichert?	□ Standleitung □ Wählleitung mit automatischem Rückruf □ Teilnehmerkennung □ 2-Faktor-Authentifizierung □ funktionelle Zuordnung einzelner Datenendgeräte	

Nr.	*Frage*	*Antwort*	*Anmerkungen*
		□ Protokollierung der Systemnutzung und Protokollauswertung □ Sonstige: _____	
3.21	Werden mobile PCs, die Daten des Auftraggebers verarbeiten bzw. speichern außerhalb der Bürozeiten unter Verschluss gehalten?	ja/nein	
3.22	Werden Räume, in denen IT-Systeme aufgestellt sind mit einem Zugangskontrollsystem ausgestattet?	ja/nein	
3.23	Wie findet die Identifizierung an IT-Systemen statt?		
3.24	Wie findet die Authentifizierung bei IT-Systemen statt?		
3.25	Wer genehmigt die Zugangsberechtigungen bei IT-Systemen?	□ benannter Systemeigentümer □ bekannter Verantwortlicher des Auftraggebers □ Sonstige: _____ □ Regelung vorhanden: ja/nein	
3.26	Werden die Zugangsberechtigungen dokumentiert?	ja/nein	
3.27	Von wem werden die Einstellungen im BIOS-Setup vorgenommen?	□ IT-Administrator □ Sonstige: _____ □ Regelung vorhanden: ja/nein	
3.28	Ist der unbefugte Zugang zum BIOS-Setup möglich?	ja/nein	
3.29	Wird bei Arbeitsunterbrechungen ein passwortgeschützter Bildschirmschoner aktiviert?	ja/nein	
3.30	Sind die Daten auf mobilen IT-Systemen verschlüsselt?	ja/nein □ komplettes System □ nur Daten	

§ 4 Zugriffskontrolle

Nr.	*Frage*	*Antwort*	*Aktivität*
4.1	Wie werden Datenträger vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen geschützt?	□ es gibt einen Verantwortlichen für Datenträgerverwaltung □ Verschlüsselung □ Biometrie □ Bestandskontrolle □ Mehraugenprinzip □ kontrollierte Vernichtung □ Anderes: _____	
4.2	Wo werden Datenträger außerhalb der Arbeitszeiten aufbewahrt?	□ Datenträgerarchiv □ verschließbare Schränke □ frei zugänglich □ an der Datenträgerverarbeitungslage □ Sonstige: _____	
4.3	Wie wird die Datenträgerverwaltung durchgeführt?		
4.4	Wird durch eine Zugriffskontrolle sichergestellt, dass Mitarbeiter(innen) nur auf Programme und Daten zugreifen können, die sie zur Aufgabenerfüllung benötigen („Need-to-know-Prinzip“)?	ja/nein	
4.5	Durch welche Maßnahmen wird die Einschränkung der Zugriffsmöglichkeit, der zur Benutzung eines IT-Systems Berechtigten auf ausschließlich die seiner Zugriffsberechtigung unterliegenden Daten gewährleistet?	□ funktionale Zuordnung einzelner Datenendgeräte □ automatische Prüfung der Zugriffsberechtigung □ Protokollierung der Zugriffsberechtigung □ Protokollierung der Systemnutzung und Protokollauswertung □ ausschließlich Menüsteuerung	
4.6	Wie ist die differenzierte Zugriffsberechtigung aufgeteilt?	□ Dateien □ Datensätze □ Datenfelder □ Anwendungsprogramme □ Betriebssystem □ Server/IT-System □ Sonstige: _____	
4.7	Wie sind die differenzierten Verarbeitungsmöglichkeiten aufgeteilt?	□ Lesen □ Ändern □ Löschen □ Sonstige: _____	
4.8	Sind die Daten auf mobilen IT-Systemen verschlüsselt?	□ ja/nein □ komplettes System □ nur Daten	

Nr.	*Frage*	*Antwort*	*Aktivität*
4.9	Können Nutzer nur auf getestete und freigegebene Anwendungssoftware zugreifen?	ja/nein □ Liste freigegebener Software	
4.10	Auf wessen Veranlassung werden Zugriffsrechte für IT-Systeme vergeben?	□ Geschäftsleitung □ disziplinarische(r) Vorgesetzte(r) □ Fachverantwortliche(r) □ Applikationsverantwortliche(r) □ Sonstige: _____ □ Regelung vorhanden: ja/nein	
4.11	Wer genehmigt die Zugriffsberechtigungen auf Daten und Applikationen?	□ Geschäftsleitung □ disziplinarische(r) Vorgesetzte(r) □ Fachverantwortliche(r) □ Applikationsverantwortliche(r) □ IT-Administrator □ Sonstige: _____ □ Regelung vorhanden: ja/nein	
4.12	Wer vergibt die Zugriffsberechtigungen im System?	□ IT-Administrator □ Sonstige: _____ □ Regelung vorhanden: ja/nein	
4.13	Werden Zugriffsrechte dokumentiert?	ja/nein	
4.14	Wie oft werden Zugriffsrechte überprüft?	□ nie □ alle ___ Wochen/Monate/Jahre	
4.15	Sind die Wechseldatenträgerlaufwerke (z. B. DVD, USB-Sticks, ext. Festplatten) gegen unbefugte Benutzung gesichert?	ja/nein □ komplettes System verschlüsselt □ nur Daten verschlüsselt	
4.16	Gibt es ein Änderungsmanagement (Changemanagement)?	ja/nein	
4.17	Wer darf die genehmigte Konfigurationsänderung vornehmen?	□ IT-Administrator □ Sonstige: _____ □ Regelung vorhanden: ja/nein	
4.18	Gibt es Sicherungsmaßnahmen gegen unbefugtes Kopieren von Daten auf lokale Rechner?	ja/nein	

§ 5 Weitergabekontrolle / Übermittlungskontrolle

Nr.	*Frage*	*Antwort*	*Anmerkungen*
5.1	Wird der Versand von Datenträgern durch Registrierung, Begleitzettel und/oder Lieferscheine kontrolliert?	ja/nein	
5.2	Besteht ein Verbot der Mitnahme von Behältnissen in Räume mit DV-Anlagen oder in Datenträgerarchive und ist das Mitbringen privater Datenträger untersagt?	Mitnahme: ja/nein Mitbringen: ja/nein	
5.3	Werden stichprobenartige Kontrollen der Mitarbeiter (Taschenkontrolle o. ä.) durchgeführt?	ja/nein	
5.4	Wo befinden sich unbenutzte Datenträger?	□ verschlossenes Behältnis □ Safe/Tresor □ Datenträgertresor □ ungeschützt □ Sonstige: _____ □ Regelung vorhanden: ja/nein	
5.5	Wie werden Datenträger vernichtet?	magnetische Datenträger: □ mehrfaches Überschreiben durch sicheres Verfahren □ physische Vernichtung □ zertifizierter Entsorger Sonstige: _____ optische Datenträger und defekte Festplatten: □ physische Vernichtung □ zertifizierter Entsorger Sonstige: Papier/Mikrofilm: □ bereitgestellte Aktenvernichter □ zertifizierter Entsorger Sonstige:	
5.6	Wie werden Datenträger transportiert?	□ unkontrolliert □ ungeschützt □ in speziellen Transportbehältnissen □ Andere:	
5.7	Wie werden Daten auf dem Übertragungsweg und beim Transport gegen das unbefugte Lesen, Kopieren, Verändern oder Entfernen geschützt?	□ Standleitung □ Wählleitung mit automatischem Rückruf □ Datenverschlüsselung	

Nr.	*Frage*	*Antwort*	*Anmerkungen*
		□ Botentransport durch Auftragnehmer/Auftraggeber □ Postversand □ verschlossen in Transportbehältern □ Transportbegleitung □ Vollständigkeits-/Richtigkeitsprüfung □ Sonstige:	
5.8	Werden Empfangsbestätigungen, Lieferschein o. ä. verwendet?	ja/nein	
5.9	Werden zum Transport vorgesehene Daten mit sensitivem Inhalt (Art. 32 DS-GVO) verschlüsselt?	Datenträger: ja/nein mobile Endgeräte: ja/nein Datenübertragungsleitungen: ja/nein	
5.10	Wird das Internet zur Weitergabe personenbezogener Daten genutzt?	ja/nein	
5.11	Welche Dienste werden dabei genutzt?	□ E-Mail □ WWW □ FTP □ elektronischer Geldverkehr □ Sonstige: _____	
5.12	Welche Sicherungsmechanismen werden bei den unter 5.11 genannten Diensten eingesetzt?	□ alle Protokolle via VPN/IP sec gesichert □ E-Mail mit SMIME oder PGP □ WWW mit https oder SSL/TLS □ SFTP □ elektronischer Geldverkehr nach PCI DSS über ZDA (PKI) □ Sonstige: _____	
5.13	Welche Sicherheitsmaßnahmen existieren?	□ Firewall □ Intrusion Detection System (IDS) □ Intrusion Prevention System (IPS) □ Virtual Private Network (VPN) □ Content Filter □ Weitere: _____	
5.14	Durch welche Maßnahmen kann überprüft und festgestellt werden, an welche Stellen Datenübermittlung durch Einrichtung zur Datenübertragung vorgesehen ist?	□ Dokumentation der vorgesehenen Abruf- und Übermittlungswege □ Dokumentation der Übermittlungsstellen und -wege □ Sonstige: _____	

Nr.	*Frage*	*Antwort*	*Anmerkungen*
5.15	Sind IT-Systeme in einem verschlossenen Raum?	ja/nein	
5.16	Sind die Server-Konsolen gesperrt?	ja/nein	
5.17	Gibt es ein Berechtigungskonzept, in dem Netzwerkfreigaben und Zugriffsberechtigungen auf Ordner und Dateien für einzelne Benutzergruppen festgelegt sind?	ja/nein □ Dokument: _____ Version/Datum: _____	
5.18	Wird das o. g. Konzept regelmäßig geprüft und aktualisiert?	□ Anzahl Prüfungen/Zeitraum: _____/_____ □ Anzahl Aktualisierungen/Zeitraum _____/_____ □ Keine Prüfung □ Keine Aktualisierung	
5.19	Werden bei Versetzung eines Mitarbeiters nicht mehr benötigte Zugangsberechtigungen entzogen?	ja/nein	
5.20	Werden bei Ausscheiden eines Mitarbeiters Zugänge zu IT-Systemen gesperrt?	ja/nein	
5.21	Welche Maßnahmen werden realisiert, wenn Rechner oder Datenträger von externen Dienstleistern mitgenommen werden müssen?	Daten werden □ logisch gelöscht □ ___ -fach überschrieben □ verschlüsselt Datenträger wird □ physisch zerstört □ vertraglich mit dem Dienstleister geregelt □ der Dienstleister belässt Datenträger auch bei Reparaturen immer beim Kunden □ Sonstige:	
5.22	Werden externe Dienstleister schriftlich auf den Datenschutz verpflichtet?	□ ja/nein □ Regelung vorhanden: ja/nein	
5.23	Wie werden geschäfts-/personenbezogene Daten bei Wartungs-/Reparaturarbeiten vor dem Zugriff durch externe Dienstleister geschützt?	□ Regelung vorhanden: ja/nein Maßnahmen: Begleitung/Beaufsichtigung □ temporär □ dauerhaft	
5.24	Werden externe Dienstleister bei ihren Aktivitäten beaufsichtigt?	ja/nein	
5.25	Werden Passwörter gewechselt, falls sie einem externen Dienstleister bekannt geworden sind?	ja/nein	

Nr.	*Frage*	*Antwort*	*Anmerkungen*
5.26	Werden die Möglichkeiten zur Fernwartung nur fallbezogen freigegeben?	ja/nein	
5.27	Wer genehmigt die Fernwartung	□ Geschäftsleitung □ verantwortlicher Abteilungsleiter □ Netzwerkadministrator □ Sonstige: _____ □ Regelung vorhanden: ja/nein	
5.28	Gibt es eine vertragliche Grundlage, die die Fernwartung regelt?	ja/nein	
5.29	Wer baut die Fernwartungsverbindung zwischen IT-Systemen und dem externen Dienstleister auf?	□ Auftraggeber initiiert Aufbau □ Netzwerkadministrator führt aus □ Sonstige: _____ □ Regelung vorhanden: ja/nein	
5.30	Gibt es einen Freigabeprozess?	ja/nein □ Regelung vorhanden: ja/nein	
5.31	Gibt es bei der Fernwartung Schutzfunktionen gegen den Zugriff eines externen Dienstleisters auf Daten/Informationen der verantwortlichen Stelle?	ja/nein welche: _____	

§ 6 Eingabekontrolle/Plausibilitätskontrolle

Nr.	*Frage*	*Antwort*	*Anmerkungen*
6.1	Durch welche Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind?	□ Erfassungsbelege mit Erfassungs- und Prüfbestätigungen □ Protokollierung eingegebener Daten □ Verarbeitungskontrolle (Transaktionskontrolle) der Anwendung □ Sonstige: _____	
6.2	Gibt es einen Schadsoftwareschutz?	ja/nein	
6.3	In welchen Intervallen wird die Integrität der Partitionstabelle, des Bootsektors, des Hauptverzeichnisses und aller Programmdateien mit einem Prüfsummenprogramm und/oder einem Schadsoftwareschutz geprüft?	täglich: □ Schadsoftwareschutz □ Prüfsummenprogramm bei jedem Rechnerstart: □ Schadsoftwareschutz □ Prüfsummenprogramm Bezeichnung: _____	
6.4	Wie und wann erfolgt ein Update des Schadsoftwareschutzes?	□ automatisch □ manuell	

Nr.	*Frage*	*Antwort*	*Anmerkungen*
		□ Sonstige: _____ □ täglich □ wöchentlich □ Sonstige: _____	
6.5	Werden sicherheitsrelevante Updates und Patches für Betriebssysteme und Anwendungsprogramme regelmäßig und zeitnah eingespielt?	ja/nein innerhalb von __ Tagen nach Veröffentlichung durch den Hersteller	
6.6	Werden Daten und Programme in unterschiedlichen Verzeichnissen abgespeichert?	ja/nein	
6.7	Werden Daten und Programme in unterschiedlichen Partitionen abgespeichert?	ja/nein	
6.8	Gibt es eine vollständige und aktuelle Netzwerkdokumentation?	ja/nein	
6.9	Wird die Integrität und Installation von erhaltenen Programmen überprüft?	ja/nein	
6.10	Werden erhaltene oder auszuliefernde Datenträger einem Schadsoftwarecheck unterzogen?	ja/nein	
6.11	Erfolgt bei Wiederverwendung bereits beschriebener Datenträger eine ausreichend starke Löschung der vorherigen Daten?	□ nein □ ja eingesetzte Software: _____ Optionen: _____	
6.12	Werden die durchgeführten Wartungs-, Fernwartungs- oder Reparaturarbeiten dokumentiert?	ja/nein	
6.13	Wird die Integrität von Datenträgern von externen Dienstleistern überprüft, bevor diese eingesetzt werden?	ja/nein	
6.14	Wird vor größeren Wartungs-, Fernwartungs- oder Reparaturarbeiten eine komplette Sicherung der betroffenen Systeme erstellt?	ja/nein	
6.15	Wird der Fernwartungsvorgang dauerhaft überprüft oder aufgezeichnet?	□ nein □ ja, durch einen Mitarbeiter der IT-Abteilung □ ja, durch Mitschnitt der Remotesession	
6.16	Findet nach den durchgeführten Wartungs-, Fernwartungs- oder Reparaturarbeiten eine Integritätsprüfung statt?	ja/nein	

§ 7 Auftragskontrolle/Vertragskonformitätskontrolle

Nr.	*Frage*	*Antwort*	*Anmerkungen*
7.1	Durch welche Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind?	□ Erfassungsbelege mit Erfassungs- und Prüfbestätigungen □ Protokollierung eingegebener Daten □ Verarbeitungskontrolle (transaktionsbasiert) □ Sonstige: _____	
7.2	Durch welche Maßnahmen wird gewährleistet, dass die Verarbeitung personenbezogener Daten im Auftrag nur entsprechend den Weisungen des Auftraggebers erfolgt?	□ schriftliche Weisung □ Angebot und Auftragsbestätigung □ Auftraggeber erhält alle Datenausgaben zur Kontrolle □ vertraglich festgelegte Verantwortlichkeiten □ Sonstige: _____	
7.3	Wie wird bei Änderungen im Verfahrensablauf/Programmänderungen durch den Auftragnehmer verfahren?	Maßnahmen:	
7.4	Wird der Auftraggeber über Programmabbrüche/Programmfehler informiert?	ja/nein	
7.5	Welche Maßnahmen werden zur Sicherung der Fernwartung/Fernadministration angewendet?	□ Ereignisauslösung vom Auftraggeber □ Rückrufautomatik □ Einmal-Passwort □ Protokollierung □ Virtual Private Network (VPN) □ Andere: _____	

§ 8 Verfügbarkeitskontrolle

Nr.	*Frage*	*Antwort*	*Anmerkungen*
8.1	Wie wird gewährleistet, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind?	□ tägliches Backup □ wöchentliches Backup □ Backup-Plan liegt vor □ SAN-Snapshots □ Festplattenspiegelung (RAID o. ä.) □ Havariearchivierung (Auslagerung) □ unterbrechungsfreie Stromversorgung (USV) □ Überspannungsfilter □ Sonstige: _____	
8.2	Gibt es Notfall und Krisenmanagement (BCM)?	ja/nein	

Nr.	*Frage*	*Antwort*	*Anmerkungen*
8.3	Gibt es ein Backup-Rechenzentrum?	ja/nein	
8.4	Wer ist für die Sicherung der Daten zuständig?	□ Auftragnehmer □ Auftraggeber □ Backup-Administrator □ Andere: _____ □ Regelung vorhanden: ja/nein	
8.5	Wie viele Generationen von Sicherungskopien existieren?	Anzahl: ___	
8.6	In welchen Intervallen wird eine Datensicherung durchgeführt?	□ täglich □ wöchentlich □ Sonstige: _____	
8.7	Wird eine regelmäßige Sicherung von datenverarbeitenden mobilen Endgeräten gewährleistet?	ja/nein	
8.8	Wird das allgemeine Backup-Verfahren regelmäßig kontrolliert?	ja/nein	
8.9	Werden Sicherungsprotokolle erstellt und geprüft?	ja/nein	
8.10	Ist das Backup-Verfahren dokumentiert?	ja/nein	
8.11	Welche Backup-Methode wird angewendet?	□ Totalsicherung □ Selektiv-Sicherung (nur Datenbestände) □ veränderte Daten	
8.12	Wo werden Backup-Medien aufbewahrt?	□ Safe/Tresor □ Datenträgertresor □ anderer Brandabschnitt □ anderes Gebäude □ im Rechenzentrum □ ungeschützt □ Sonstige: _____ □ Regelung vorhanden: ja/nein	
8.13	Werden gesetzliche Aufbewahrungsfristen beachtet?	ja/nein	
8.14	Werden die gesetzlichen Vorgaben zur Löschung, Einschränkung und dem „Recht auf Vergessen werden“ eingehalten?	ja/nein	
8.15	Werden E-Mails, die die Geschäftsbeziehung mit dem Auftraggeber betreffen bzw. Daten enthalten, die für die Auftragsabwicklung notwendig sind, regelmäßig archiviert?	ja/nein	
8.16	Wie werden E-Mails archiviert?	□ automatisch durch: _____ □ zentral durch Administratoren □ zentral durch Archivsystem	
8.17	Ist das Archivsystem zertifiziert?	ja/nein	

Nr.	*Frage*	*Antwort*	*Anmerkungen*
		zertifiziert durch: _____	
8.18	Welche störenden Einflüsse existieren beim Auftragnehmer in Räumen bzw. Gebäuden, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet?	□ Hitze, Kälte, Feuchtigkeit □ HF-Strahlung und elektromagnetische Kraftfelder □ Bahnanlagen □ Stromausfall oder Stromschwankungen während des laufenden Betriebs □ Sonstige: _____	
8.19	Werden schädigende Umgebungseinflüsse in Räumen bzw. Gebäuden, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet, bei der Installation und der Benutzung von IT-Komponenten beachtet?	ja/nein	
8.20	Gibt es eine Risikobewertung und einen Risikobehandlungsplan?	ja/nein	
8.21	Gibt es in den Serverräumen wasserführende Leitungen oder leichtbrennbare oder entzündliche Gegenstände?	□ ja, wassergekühlte Schranksysteme □ ja, wasserführende Leitungen □ ja, leichtbrennbare Gegenstände □ nein	
8.22	Sind in den Serverräumen Feuchtigkeits-, Rauch-, Wärmesensoren installiert?	□ Brandmelder □ Rauchansaugsystem □ Feuchtigkeitssensoren □ Wärmesensoren □ Leckagemelder □ Weitere: _____	
8.23	Stehen in den Serverräumen entsprechend zugelassene Feuerlöscher /Löschanlagen zur Verfügung?	ja/nein	
8.24	Wie wird ein zuständiger Mitarbeiter bei einem Alarmsignal eines Sensors über den kritischen Zustand in den Serverräumen des Rechenzentrums informiert?	□ Telefon □ SMS □ Anderes: _____	
8.25	Ist die Erreichbarkeit eines zuständigen Mitarbeiters im Katastrophenfall jederzeit gewährleistet?	ja/nein □ Rufbereitschaft □ 24/7 Betrieb	
8.26	Gibt es Eskalationspläne?	ja/nein	
8.27	Sind die Serverräume vor Einbruch ausreichend geschützt?	ja/nein	
8.28	Sind die Serverräume entsprechend der technischen Spezifikation ausreichend klimatisiert?	ja/nein	
8.29	Stehen die Server in 19“-Racks?	ja/nein	
8.30	Mit welcher Tür sind die Serverräume ausgestattet?	□ normale Tür □ feuersichere Tür □ Stahltür	

Nr.	*Frage*	*Antwort*	*Anmerkungen*
		□ Andere: _____	
8.31	Werden verfahrensfremde Datenträger mit eindeutiger Zuordnung verwaltet?	ja/nein	
8.32	Besteht eine Archivordnung?	ja/nein	
8.33	Ist ein Archivverwalter bestellt?	ja/nein	
8.34	Existiert ein eigener Archivraum (Sicherungsbereich)?	ja/nein	
8.35	Besteht lediglich ein beschränkter Zugang zum Archivbereich?	ja/nein	
8.36	Erfolgt die Ein- und Ausgabe von Datenträgern nur durch die Archivverwaltung?	ja/nein	
8.37	Wird die Ein- und Ausgabe von Datenträgern revisionsfähig protokolliert?	ja/nein	
8.38	Erfolgen regelmäßige Bestandskontrollen der Datenträger durch Soll-/Ist-Vergleich?	ja/nein	
8.39	Ist das Mitnehmen von Taschen und Mänteln in die Sicherheitszonen (Archiv) untersagt?	ja/nein	
8.40	Ist das Mitnehmen von Telefonen, Fotoapparaten und anderen elektronischen Geräten in Sicherheitszonen (Archiv) untersagt?	ja/nein	
8.41	Wer ist für die Einhaltung von Wartungsintervallen, der Auswahl und Beauftragung von Wartungsunternehmen verantwortlich?	□ IT-Leitung □ IT-Administrator □ Fachvorgesetzter □ Sonstige: _____ □ Regelung vorhanden: ja/nein	

§ 9 Datentrennungskontrolle/Mandantentrennungskontrolle

Nr.	*Frage*	*Antwort*	*Anmerkungen*
9.1	Wie wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können?	□ softwareseitiger Ausschluss (Mandantentrennung) □ Dateiseparierung □ Datenbankprinzip (Trennung über Zugriffsregelungen) □ eigene Datenbankinstanz □ Trennung von Test- und Routineprogrammen □ Trennung von Test- und Produktivdaten □ eigene IT-Systeme je Auftraggeber □ Sonstige: _____	
9.2	Aus welchen Gründen ist eine Trennung nicht möglich/notwendig?		

§ 10 Prüfung der Betriebsorganisation und Rechenschaftspflicht

Nr.	*Frage*	*Antwort*	*Anmerkungen*
10.1	Durch welche Maßnahmen ist die innerbetriebliche Organisation so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird?	□ Verfahrensregister beim Auftraggeber sind vorhanden, vollständig, aktuell □ Verfahrensregister beim Auftragnehmer sind vorhanden, vollständig, aktuell □ Nachweise über durchgeführte Schulungen der Mitarbeiter zum Datenschutz liegen vor □ Nachweise über Einhaltung der datenschutzrechtlichen Verpflichtungen der verarbeitenden Mitarbeiter liegen vor □ Datenschutzbeauftragter ist schriftlich bestellt □ Fachkundenachweise des Datenschutzbeauftragten liegen vor □ Stellenbeschreibung für den Datenschutzbeauftragten liegt vor □ Datenschutzordnung liegt vor □ Sicherheitskonzept liegt vor □ Sicherheitskonzept wird regelmäßig aktualisiert □ schriftliche Arbeitsanweisungen/Richtlinien/Merkblätter liegen vor □ Programme/Verfahren sind ordnungsgemäß dokumentiert □ Aufbewahrung/Archivierung aller maschinell erzeugten Protokolle ist geregelt □ Programmfreigabeverfahren ist eingerichtet □ Datenschutzfolgen-Abschätzung gem. Art. 35 DS-GVO wurden durchgeführt und protokolliert □ Funktionstrennung im IT-Bereich existiert □ Abstimm- und Kontrollverfahren sind eingerichtet	

Nr.	*Frage*	*Antwort*	*Anmerkungen*
		□ Vier-Augen-Prinzip wird angewendet bei: □ Es ist sichergestellt, dass bei der Übermittlung personenbezogener Daten außerhalb der EU in Drittstaaten ein angemessenes Datenschutzniveau nach Art. 44, 46, 49 DS-GVO eingehalten wird. □ Einwilligungen Art. 6 Abs. 1 lit. a bis f DS-GVO liegen vor □ Benachrichtigungen, Auskunftsersuchen, Anliegen bezüglich Berichtigung, Löschung oder Sperrung wurden dokumentiert □ ordnungsgemäßer Einsatz von Video-/Web-Kameras ist gesichert □ ordnungsgemäßer Einsatz von Chipkartentechnik, Biometrie oder ähnlicher Technologien ist gesichert □ es existiert ein Bereich Revision, der auch den Datenschutz abdeckt □ weitere Punkte:	

Abbildung 27: Formular technisch organisatorische Maßnahmen[1242]

1242 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, S. 460, Rn. 1 - 56, Art. 32, 25 DSGVO.

V. Fragebogen Basisauditierung

Nr.	*Frage*	*Anm. Auditor*
1	***Unternehmen***	
1.1	Bitte legen Sie ein aktuelles Organigramm des Unternehmens oder der Unternehmensgruppe vor.	
1.2	Benennen Sie sämtliche Standorte Ihres Unternehmens jeweils mit Angabe der wesentlichen am Standort stattfindenden Datenverarbeitungen (Stichworte).	
1.3	Befinden sich Standorte des Unternehmens außerhalb der EU oder des Europäischen Wirtschaftsraumes („EWR“)?	
1.4	Sofern es Standorte außerhalb der EU oder des EWR gibt, erfolgt mit diesen Standorten ein Austausch von Daten oder eine gemeinsame Nutzung von IT-Ressourcen?	
1.5	Geben Sie die Anzahl der Mitarbeiter Ihres Unternehmens an, bei mehreren Standorten bitte auch pro Standort. Differenzieren Sie nach fest angestellten Mitarbeitern, Auszubildenden, Aushilfen, Praktikanten, Studenten etc.	
1.6	Benennen Sie Produkte und Dienstleistungen Ihres Unternehmens und erläutern Sie diese stichwortartig.	
1.7	Werden im Unternehmen – außerhalb der Personalabteilung – besondere Arten personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) verarbeitet?	
1.8	Werden im Unternehmen automatisierte Einzelfallenscheidungen mit unmittelbarer Wirkung für den Betroffenen getroffen?	
1.9	Verarbeitet das Unternehmen (auch) personenbezogene Daten von Kindern? Falls ja, auf welcher Rechtsgrundlage erfolgt die Verarbeitung?	
1.10	Besteht in Ihrem Unternehmen oder der Unternehmensgruppe ein Betriebsrat?	
2	***Datenschutzdokumentation***	
2.1	Bitte legen Sie das aktuelle Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO) vor.	
2.2	Falls das Verzeichnis von Verarbeitungstätigkeiten unvollständig ist oder nicht existiert, benennen Sie bitte die Abteilungen und Prozesse im Unternehmen, die mit personenbezogenen Daten umgehen.	
2.3	Sofern konzernverbundene Unternehmen mit personenbezogenen Daten des Unternehmens umgehen, legen Sie bitte die entsprechenden Vereinbarungen nach Art. 28 DS-GVO vor oder benennen Sie die Rechtsgrundlage für die Übermittlung.	
2.4	Legen Sie bitte eine Liste aller Dienstleister vor, die für Sie im Rahmen einer Auftragsverarbeitung tätig sind und fügen Sie die abgeschlossenen Verträge zur Auftragsverarbeitung bei. Vermerken Sie bitte – soweit bekannt – jeweils, wenn der Vertrag ganz oder teilweise auf Standardvertragsklauseln (Art. 28 Abs. 7, 8 DS-GVO) beruht, ob sich der Auftragsverarbeiter zur Einhaltung genehmigter Verhaltensregeln (Art. 40 DS-GVO) verpflichtet hat und/oder gem. Art. 42 DS-GVO zertifiziert ist.	

Nr.	*Frage*	*Anm. Auditor*
2.5	Bitte legen Sie von den Auftragsverarbeitern bereitgestellte Unterlagen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DS-GVO vor.	
2.6	Falls die Liste der Auftragsverarbeiter unvollständig ist oder nicht existiert, übergeben Sie dem Auditor bitte eine Liste der Unternehmen und Dienstleister, die für Sie Datenverarbeitungen vornehmen (inkl. Wartung von Datenverarbeitungsanlagen).	
2.7	Wie wird im Unternehmen sichergestellt, dass die Mitarbeiter, die Zugang zu personenbezogenen Daten haben, diese nur nach Weisung des Verantwortlichen verarbeiten?	
2.8	Verfügt das Unternehmen über ein Datenschutzmanagementsystem und wird dieses aktiv genutzt?	
2.9	Bestehen Zertifizierungen nach Art.42 DS-GVO?	
3	***Datenschutzorganisation***	
3.1	Ist im Unternehmen ein Datenschutzbeauftragter („DSB“) bestellt? Falls ja, teilen Sie bitte die Kontaktdaten mit und machen Sie Angaben zur Qualifikation des DSB.	
3.2	Falls kein DSB bestellt ist: Bitte legen Sie unter Berücksichtigung von Art. 37 DS-GVO und nationaler Regelungen zum Datenschutzbeauftragten dar, warum eine Bestellung nicht erforderlich ist.	
3.3	Wenn ein DSB bestellt ist: Wie wird sichergestellt, dass er über neue Verfahren oder Änderungen bestehender Verfahren frühzeitig informiert wird?	
3.4	Wie ist organisatorisch sichergestellt, dass vor jeder Verarbeitung von personenbezogenen Daten geprüft wird, ob die geplante Verarbeitung zulässig ist?	
3.5	Besteht ein Prozess für die Durchführung und Dokumentation von Datenschutz-Folgenabschätzungen?	
3.6	Wie ist im Unternehmen sichergestellt, dass die Informationspflichten gegenüber den Betroffenen vollständig und rechtzeitig erfüllt werden?	
3.7	Wie werden im Unternehmen die Grundsätze des „Datenschutz durch Technikgestaltung“ (Privacy-by-design) und der „datenschutzfreundlichen Voreinstellungen“ (Privacy-by-default) umgesetzt?	
3.8	Hat das Unternehmen ein Datenschutzkonzept? Falls ja: Bitte vorlegen.	
3.9	Gibt es im Unternehmen ein aktuelles Rollen- und Rechtekonzept?	
3.10	Wer legt im Unternehmen fest, welche (Zugriffs-)Rechte Mitarbeiter bei Einstellungen oder Versetzungen erhalten und welche ggf. entzogen werden müssen?	
3.11	Erfolgt die organisatorische Rechtebewilligung getrennt von der technischen Rechteeinräumung? Wie wird dokumentiert, welche Rechte ein User erhält?	
3.12	Besteht ein standardisierter Prozess beim Ausscheiden von Mitarbeitern?	

Nr.	*Frage*	*Anm. Auditor*
3.13	Ist die private Nutzung von Internetzugang, E-Mail-Postfach, dienstlichem Telefon und ggf. weiteren dienstlichen Geräten klar geregelt? Bitte Regelung vorlegen.	
3.14	Wie wird bei einem bestehenden Verbot der privaten Nutzung von Internetzugang, E-Mail-Postfach, dienstlichem Telefon und weiteren dienstlichen Geräten die Einhaltung des Verbots kontrolliert?	
3.15	Besteht ein Prozess zur Beauftragung externer Dienstleister, die mit personenbezogenen Daten umgehen? Bitte legen Sie eine Prozessbeschreibung vor.	
3.16	Wer legt die Anforderungen an die technischen und organisatorischen Maßnahmen fest, die externe Dienstleister einzuhalten haben?	
3.17	Existiert ein dokumentierter Prozess zum Umgang mit Auskunftsverlangen nach Art. 15 DS-GVO? Bitte legen Sie die Prozessbeschreibung vor.	
3.18	Wie wird das Recht auf Datenübertragbarkeit vom Unternehmen sichergestellt? Besteht ein entsprechender Prozess?	
3.19	Wie ist sichergestellt, dass Forderungen Betroffener nach Berichtigung, Löschung oder Einschränkung der Verarbeitung von personenbezogenen Daten geprüft und umgesetzt werden können?	
3.20	Sofern personenbezogene Daten öffentlich gemacht wurden: Welche Prozesse sind implementiert, wenn Betroffene ihr Recht auf Vergessenwerden gelten machen?	
3.21	Wie werden Widersprüche Betroffener gegen Datenverarbeitungen auf Grundlage einer Interessenabwägung vom Unternehmen geprüft und umgesetzt?	
3.22	Wie ist die Einhaltung der gesetzlichen Archivierungs- und Löschungsfristen im Unternehmen sichergestellt?	
3.23	Besteht ein Maßnahmenplan für den Fall, dass der Schutz personenbezogener Daten verletzt wird (Art. 33, 34 DS-GVO)?	
3.24	Wie erfolgt die regelmäßige Unterrichtung der Beschäftigten zu Datenschutzthemen? Besteht ein Schulungsplan?	
4	***IT-Systeme***	
4.1	Bitte legen Sie eine Übersicht über die IT-Infrastruktur und alle Systeme vor, auf denen personenbezogene Daten verarbeitet werden.	
4.2	Bitte benennen Sie, sofern nicht in 4.1 enthalten, die zentralen Standorte von Datenverarbeitungssystemen und deren Hauptaufgaben.	
4.3	Werden die Standorte regelmäßig einer externen Prüfung unterzogen (z. B. ISO 27001, IT-Grundschutz, geprüftes Rechenzentrum)? Bitte legen Sie die jeweils aktuellen Prüfberichte vor.	
4.4	Unterziehen Sie Systeme regelmäßigen Sicherheitsüberprüfungen (z. B. Penetration-Tests oder Security Audit Trails)? Bitte legen Sie aktuelle Prüfberichte oder Logs vor.	

Nr.	*Frage*	*Anm. Auditor*
4.5	Setzen Sie eine zentrale Unternehmenssoftware (ERP-System) ein? Falls ja, welche?	
4.6	Sofern Sie eine ERP-Software einsetzen, wird diese auf eigenen Systemen (intern oder Housing), auf fremden Systemen (Hosting) oder als SaaS-Lösung betrieben?	
4.7	Besteht ein externer Zugriff auf einzelne oder alle Systeme im Netzwerk (z. B. für Home Office, E-Mail-Abruf oder Fernwartung)? Bitte listen Sie auf, welche Nutzergruppen auf welche Systeme Zugriff haben und wie dieser Zugriff abgesichert wird.	
4.8	Können Mitarbeiter auf Ihren Clients, Laptops oder Tablets eigenständig Software installieren?	
4.9	Werden die Festplatten/Speichereinheiten mobiler Geräte verschlüsselt?	
4.10	Setzen Sie ein Mobile Device Management ein? Falls ja, welches?	
4.11	Nutzt das Unternehmen oder nutzen Mitarbeiter und Abteilungen Cloud-Speicherdienste wie Google Drive, Dropbox oder Microsoft OneDrive?	
4.12	Nutzt das Unternehmen Cloud-Services wie Salesforce (CRM), Datapine (Data Analytics) oder ähnliche Dienste?	
4.13	Besteht ein IT-Sicherheitskonzept? Bitte legen Sie dieses vor.	

Abbildung 28: Fragebogen Basisauditierung[1243]

1243 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, S. 141, Bertermann/Piltz - Fragebogen Datenschutzaudit.

VI. Muster-Vorlage Verarbeitungstätigkeiten

§ 1

Beschreibung und Identifizierungs-merkmale
detaillierte Beschreibung
Schnittstellen und Peripheriegeräte
Standort oder Name des Beschäftigten
damit ausgeführte Verfahren

§ 2

Namen und Kontaktdaten des Verantwortlichen	
Namen und Kontaktdaten des Datenschutzbeauftragten	
Namen und Kontaktdaten eines ggf. vorhandenen Vertreters	
laufende Nummer der Verarbeitungstätigkeit	1 / 2
Zwecke der Verarbeitung	
Namen und Kontaktdaten eines ggf. vorhandenen gemeinsam Verantwortlichen	
Kategorien betroffener Personen:	
Kategorien von Daten bzw. Datenarten	
Regelfristen für die Löschung	
Kategorien von Empfängern	
das Drittland oder die internationale Organisation, an das oder die ggf. übermittelt wird, sowie ggf. die Dokumentierung geeigneter Garantien	
allgemeine Beschreibung der Maßnahmen gem. Art. 32 Abs. 1 DS-GVO	

§ 3

laufende Nummer der im Auftrag ausgeführten Verarbeitungstätigkeiten	A1	A2
Namen und Kontaktdaten des Verantwortlichen und seines Datenschutzbeauftragten		
Namen und Kontaktdaten eines ggf. gleichzeitig mitbeauftragten Auftragsverarbeiters		
Kategorien von Verarbeitungen		
das Drittland oder die internationale Organisation, an das oder die ggf. übermittelt wird, sowie ggf. die Dokumentierung geeigneter Garantien		
allgemeine Beschreibung der Maßnahmen gem. Art. 32 Abs. 1 DS-GVO		

Abbildung 29: Muster Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO) [1244]

1244 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, S. 157 und 158, Benennung von Verarbeitungstätigkeiten nach Art. 30 DSGVO.

VII. Muster-Formular Zielvereinbarung

„Muster“ Zielvereinbarungen dokumentieren

Jahr		**Bereich**	
Name Mitarbeiter/in		Sonst. Angaben zur Person	
Name Vorgesetzter/in		Sonst. Angaben zur Person	
Zielvereinbarungen gemäß Gespräch vom:			
Ziele Mitarbeiter/in	**Teilziele und Aktivitäten**	**Ziel erreicht, wenn**	**Termin**
Notwendige Rahmenbedingungen		**Fördermaßnahmen / Qualifizierung**	
Anmerkungen / sonstiges			
Ich erkläre mich mit den Zielvereinbarungen einverstanden.			
Datum		Uhrzeit	
Unterschrift Mitarbeiter/in		Unterschrift Vorgesetzte/r	

Abbildung 30: Formular zur Zielvereinbarung

VIII. Muster-Vorlage Datenschutzerklärung für Webseiten

Datenschutzerklärung

§ 1 Information über die Erhebung personenbezogener Daten

(1) Im Folgenden informieren wir [Unternehmen / Betreiberüber] die Erhebung personenbezogener Daten bei Nutzung unserer Website. Personenbezogene Daten sind alle Daten, die auf Sie persönlich beziehbar sind, z. B. Name, Adresse, E-Mail-Adressen, Nutzerverhalten.

(2) Verantwortlicher gem. Art. 4 Abs. 7 EU-Datenschutz-Grundverordnung (DS-GVO) ist [Name, ladungsfähige Anschrift, E-Mail-Adresse] (siehe unser Impressum). [Unseren Datenschutzbeauftragten erreichen Sie unter [Datenschutz@example.com] oder unserer Postadresse mit dem Zusatz „der Datenschutzbeauftragte".]

(3) Bei Ihrer Kontaktaufnahme mit uns per E-Mail oder über ein Kontaktformular werden die von Ihnen mitgeteilten Daten (Ihre E-Mail-Adresse, ggf. Ihr Name und Ihre Telefonnummer) von uns gespeichert, um Ihre Fragen zu beantworten. Die in diesem Zusammenhang anfallenden Daten löschen wir, nachdem die Speicherung nicht mehr erforderlich ist, oder schränken die Verarbeitung ein, falls gesetzliche Aufbewahrungspflichten bestehen.

(4) Falls wir für einzelne Funktionen unseres Angebots auf beauftragte Dienstleister zurückgreifen oder Ihre Daten für werbliche Zwecke nutzen möchten, werden wir Sie untenstehend im Detail über die jeweiligen Vorgänge informieren. Dabei nennen wir auch die festgelegten Kriterien der Speicherdauer.

§ 2 Ihre Rechte

(1) Sie haben gegenüber uns folgende Rechte hinsichtlich der Sie betreffenden personenbezogenen Daten:

- Recht auf Auskunft,
- Recht auf Berichtigung oder Löschung,
- Recht auf Einschränkung der Verarbeitung,
- Recht auf Widerspruch gegen die Verarbeitung,
- Recht auf Datenübertragbarkeit.

(2) Sie haben zudem das Recht, sich bei einer Datenschutz-Aufsichtsbehörde über die Verarbeitung Ihrer personenbezogenen Daten durch uns zu beschweren.

§ 3 Erhebung personenbezogener Daten bei Besuch unserer Website

(1) Bei der bloß informatorischen Nutzung der Website, also wenn Sie sich nicht registrieren oder uns anderweitig Informationen übermitteln, erheben wir nur die personenbezogenen Daten, die Ihr Browser an unseren Server übermittelt. Wenn Sie unsere Website betrachten möchten, erheben wir die folgenden Daten, die für uns technisch erforderlich sind, um Ihnen unsere Website anzuzeigen und die Stabilität und Sicherheit zu gewährleisten (Rechtsgrundlage ist Art. 6 Abs. 1 S. 1 lit. f DS-GVO):

- IP-Adresse
- Datum und Uhrzeit der Anfrage
- Zeitzonendifferenz zur Greenwich Mean Time (GMT)
- Inhalt der Anforderung (konkrete Seite)
- Zugriffsstatus/HTTP-Statuscode
- jeweils übertragene Datenmenge
- Website, von der die Anforderung kommt
- Browser
- Betriebssystem und dessen Oberfläche
- Sprache und Version der Browsersoftware.

(2) Zusätzlich zu den zuvor genannten Daten werden bei Ihrer Nutzung unserer Website Cookies auf Ihrem Rechner gespeichert. Bei Cookies handelt es sich um kleine Textdateien, die auf Ihrer Festplatte dem von Ihnen verwendeten Browser zugeordnet gespeichert werden und durch welche der Stelle, die den Cookie setzt (hier durch uns), bestimmte Informationen zufließen. Cookies können keine Programme ausführen oder Viren auf Ihren Computer übertragen. Sie dienen dazu, das Internetangebot insgesamt nutzerfreundlicher und effektiver zu machen.

(3) Einsatz von Cookies:

a) Diese Website nutzt folgende Arten von Cookies, deren Umfang und Funktionsweise im Folgenden erläutert werden:

- Transiente Cookies (dazu b),
- Persistente Cookies (dazu c).

b) Transiente Cookies werden automatisiert gelöscht, wenn Sie den Browser schließen. Dazu zählen insbesondere die Session-Cookies. Diese speichern eine sogenannte Session-ID, mit welcher sich verschiedene Anfragen Ihres Browsers der gemeinsamen Sitzung zuordnen lassen. Dadurch kann Ihr Rechner wiedererkannt werden, wenn Sie auf unsere Website zurückkehren. Die Session-Cookies werden gelöscht, wenn Sie sich ausloggen oder den Browser schließen.

c) Persistente Cookies werden automatisiert nach einer vorgegebenen Dauer gelöscht, die sich je nach Cookie unterscheiden kann. Sie können die Cookies in den Sicherheitseinstellungen Ihres Browsers jederzeit löschen.

d) Sie können Ihre Browser-Einstellung entsprechend Ihren Wünschen konfigurieren und z. B. die Annahme von Third-Party-Cookies oder allen Cookies ablehnen. Wir weisen Sie darauf hin, dass Sie eventuell nicht alle Funktionen dieser Website nutzen können.

e) [Wir setzen Cookies ein, um Sie für Folgebesuche identifizieren zu können, falls Sie über einen Account bei uns verfügen. Andernfalls müssten Sie sich für jeden Besuch erneut einloggen.]

f) [Die genutzten Flash-Cookies werden nicht durch Ihren Browser erfasst, sondern durch Ihr Flash-Plug-in. Weiterhin nutzen wir HTML5 storage objects (Objektspeicherung), die auf Ihrem Endgerät abgelegt werden. Diese Objekte speichern die erforderlichen Daten unabhängig von Ihrem verwendeten Browser und haben kein automatisches Ablaufdatum. Wenn Sie keine Verarbeitung der Flash-Cookies wünschen, müssen Sie ein entsprechendes Add-On installieren, z. B. „Better Privacy“ für Mozilla Firefox (https://addons.mozilla.org/de/firefox/addon/betterprivacy/) oder das Adobe-Flash-Killer-Cookie für Google Chrome. Die Nutzung von HTML5 storage objects können Sie verhindern, indem Sie in Ihrem Browser den privaten Modus einsetzen. Zudem empfehlen wir, regelmäßig Ihre Cookies und den Browser-Verlauf manuell zu löschen.]

IX. Muster-Richtlinie und Betriebsvereinbarung zur Videoüberwachung

§ 1 Geltungsbereich und Gegenstand

Diese Richtlinie regelt, unter welchen Voraussetzungen im [Unternehmen] Videoüberwachung in Innen- und Außenbereichen eingesetzt werden und eine Auswertung erfolgen darf. Sie gilt für alle Beschäftigten [und Beamte] des Unternehmens in [der /den Niederlassung/en …].

[ODER, bei Betriebsvereinbarungen:

1. Diese Richtlinie regelt, unter welchen Voraussetzungen im [Unternehmen] Videoüberwachung eingesetzt werden und eine Auswertung der Aufnahmen erfolgen darf. Sie gilt für alle Arbeitnehmerinnen und Arbeitnehmer, die dem Betrieb […] angehören. Für alle Mitarbeiterinnen und Mitarbeiter, die nicht unter den Arbeitnehmerbegriff des § 5 BetrVG fallen, wird eine Videoüberwachung nach den identischen Vorgaben dieser Betriebsvereinbarung, sowie § 26 BDSG n. F., Art. 88 DS-GVO sichergestellt. Nachfolgend werden alle erfassten Personen gemeinsam als „Beschäftigte“ bezeichnet.]

2. Der Begriff Videoüberwachung umfasst in dieser Richtlinie den Betrieb aller Videokameras, soweit Anbringung und/oder Betrieb auf Veranlassung von oder durch [Unternehmen] erfolgen. Erfasst sind rein übertragende („Monitoring“) ebenso wie aufzeichnende Systeme, Kamera-Attrappen sowie noch nicht und nicht mehr funktionsfähige Kameras.

3. Eine Leistungskontrolle durch die Videoüberwachung ist unzulässig. Eine Verhaltens- oder Anwesenheitskontrolle ist nur zulässig, soweit es die in Anlage 1 festgelegte Zweckbestimmung gestattet.

4. Die Richtlinie umfasst nicht solche Videosysteme, die allein der Überwachung von technischen Abläufen dienen. Dies gilt jedoch nur, wenn ausgeschlossen ist, dass Personen erfasst werden und/oder Rückschlüsse auf das Arbeitsverhalten von Beschäftigten möglich sind. Diese Kamerasysteme sind ohne Zoom-, Schwenk- oder Aufnahmefunktion fest zu installieren.

5. Die Richtlinie gilt nicht bei der Kommunikation dienenden Systemen, also insbesondere Webcams, Bildschirmarbeitsplätze und Videokonferenzen.

§ 2 Umfang und Zweck der Videoüberwachung

1. Die Videoüberwachung erfolgt in den gesetzlichen Grenzen, insbesondere des Bundesdatenschutzgesetzes (BDSG n. F.) und der EU-Datenschutz-Grundverordnung (DS-GVO). Die Videoüberwachung darf nur das Betriebsgelände erfassen, keinen öffentlichen Straßenraum.

2. Vor der Installation eines Kamera-Systems ist eine Dokumentation von Zweck und Grund der Videoüberwachung in dem in Anlage 1 dargestellten Formblatt schriftlich festzulegen. Die Videoüberwachung ist nur zulässig, soweit es die Interessen von [Unternehmen] erfordern und keine berechtigten Interessen der Beschäftigten oder außenstehender Personen entgegenstehen. Die Erforderlichkeit zur Erreichung der Zwecke ist grundsätzlich anhand der Tabelle 1 für jede Kamera gesondert zu prüfen. Der Kamerabetrieb ist ausschließlich zu den vor Inbetriebnahme festgelegten Zwecken zulässig. [ZUSÄTZLICH, bei Betriebsvereinbarungen: Das Formblatt ist dem Betriebsrat vor Einsatz des Kameras-Systems zur Prüfung vorzulegen. Diese Betriebsvereinbarung dient zudem der Erfüllung des Mitbestimmungsrechts des Betriebsrats nach § 87 Abs. 1 Ziff. 6 BetrVG. Nach dem übereinstimmenden Willen der Parteien stellt diese Betriebsvereinbarung eine anderweitige Rechtsvorschrift dar, die eine Datenverarbeitung gestattet.]

3. Im Innenbereich, also innerhalb der Gebäude-Außenwände, ist die Videoüberwachung während der Betriebszeiten [Uhrzeit] nur bei Vorliegen eines auf konkrete Personen bezogenen Verdachts einer strafbaren Handlung zulässig. Diese Feststellungen, die den konkreten Verdacht einer strafbaren Handlung gegenüber bestimmten Personen begründen, beispielsweise Sachbeschädigungen oder abhandenkommendes Eigentum, sind im Formblatt Anlage 1 schriftlich zu dokumentieren. [ZUSÄTZLICH, bei Betriebsvereinbarungen: Diese Informationen sind dem Betriebsrat vor Inbetriebnahme vorzulegen und unterliegen der Geheimhaltungspflicht des § 79 BetrVG.] Die Überwachung ist auf den räumlichen Bereich zu beschränken, dem der konkrete Verdacht zugeordnet werden kann. Eine verdachtsunabhängige, rein präventive Inbetriebnahme der Überwachungsanlage ist unzulässig. Es sind maximal [sechs] Kameras einzusetzen. An einem konkreten Ort ist die Überwachung höchstens [vier Wochen] lang zulässig. Die Dauer der Videoaufzeichnung ist auf den erforderlichen Umfang zu beschränken. Sie ist

unverzüglich einzustellen, sobald das Ziel erreicht wurde. Außerhalb der Betriebszeiten ist die Innenüberwachung mit Aufzeichnung zulässig, soweit die Voraussetzungen dieser Richtlinie eingehalten sind.

4. Eine verdeckte Videoüberwachung von Beschäftigten darf nur durchgeführt werden, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des [Unternehmens] besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind und die verdeckte Videoüberwachung damit praktisch das einzig verbleibende Mittel zur Aufklärung der Straftaten darstellt. Dies ist vor Inbetriebnahme im Formblatt Anlage 1 darzulegen und dabei insgesamt eine Verhältnismäßigkeitsprüfung durchzuführen. Die verdeckte Videoüberwachung ist in diesen Einzelfällen nur gegen einen zuvor festgelegten räumlich und funktional abgrenzbaren Kreis von Arbeitnehmern durchzuführen.

5. Im Außenbereich (das Betriebsgelände zwischen Gebäudetüren und Außenzaun) ist eine dauerhafte Videoüberwachung auch während der Betriebszeiten zulässig, soweit die Voraussetzungen dieser Richtlinie eingehalten sind.

6. Eine Videoüberwachung von Ruhebereichen, Pausenräumen oder Umkleidekabinen findet nicht statt.

§ 3 Technische Einschränkung der Videoüberwachung

1. Alle verwendeten Kamerasysteme sind in der als Anlage 2 dargestellten Tabelle aufzuführen, wobei Art des Systems, Leistungsmerkmale (Reichweite, Zoomfunktion, Schwenkfunktion usw.) sowie Anzahl und Standorte der Kameras, Aufzeichnungsgeräte, Monitore und weiterer technischer Geräte zu dokumentieren sind.

2. Es sind grundsätzlich nur fest installierte Kameras ohne Zoom- oder Schwenkfunktion einzusetzen. Ausnahmen sind nur im Außenbereich zulässig, soweit keine Arbeitsplätze erfasst werden.

3. Regelmäßig ist vorrangig zu prüfen, ob automatisierte Sichtfeld-Einschränkungen vorgenommen werden können und ob ein automatisiertes Ausblenden oder Verpixeln von Personen implementiert werden kann. Für aufzeichnende Systeme gelten ergänzend die Regelungen des § 5.

4. Nicht erforderliche Funktionen der Systeme, z. B. Mikrofone oder eine lokale Speicherung von Daten, sind vorrangig dauerhaft, ansonsten temporär zu deaktivieren.

5. Die jeweiligen Prüfungen, insbesondere Gründe der Nichtimplementierung von Schutzmaßnahmen, sind in dem Formblatt Anlage 1 zu dokumentieren.

6. Eine akustische Überwachung findet nicht statt.

7. Bei allen Videoaufnahmen ist stets die Datums- und Zeitangabe im Bild einzublenden.

8. Die jeweiligen Kamerasysteme sind getrennt voneinander zu betreiben und, soweit möglich, nicht mit sonstigen IT-Systemen zu verknüpfen. Die Datenübertragung hat, soweit technisch möglich, verschlüsselt zu erfolgen. Es ist das in Anlage 2 dokumentierte Berechtigungskonzept mit kontinuierlicher Pflege der Berechtigungen zu führen.

9. Ein Abgleich von Kamerabildern mit einer Bilddatenbank ist nur in begründeten Einzelfällen zulässig, insbesondere wenn eine Handlung entdeckt wird, die laut dem Zweck der Videoüberwachung erfasst werden soll. Der Abgleich hat im Beisein des Datenschutzbeauftragten [und des Betriebsrates] zu erfolgen. Werden bei Auswertung der Aufnahmen bzw. dem Abgleich mit der Bilddatenbank einzelne Personen identifiziert, sind diese per E-Mail oder Post zu informieren.

10. Jede Änderung der Standorte und der Anzahl der Kameras sowie jede technische Leistungsänderung, die den Betrieb der Videoanlage, ihre Nutzung, die Speicherung von Daten und/oder deren Auswertung betrifft, bedarf der Zustimmung des Betriebsrats.]

§ 4 Technisch-organisatorische Sicherheit

1. Die Einrichtung der Videoüberwachungsanlage ist durch eine spezialisierte Firma unter Aufsicht des Datenschutzbeauftragten vorzunehmen.

2. Bei Durchführung einer Videoüberwachung sind regelmäßig die gesetzlich vorgeschriebenen technischen und organisatorischen Maßnahmen zu beachten (Art. 32 DS-GVO). Diese werden dargestellt in [der Konzernrichtlinie].

3. Der Zugang zu den Daten ist grundsätzlich nur Personen unter ihren persönlichen Zugangsdaten zu gewähren, die vorher namentlich festgelegt wurden. Es sollten,

soweit möglich, nur betriebsinterne Personen gewählt werden oder Mitarbeiter eines externen Sicherheitsunternehmens (wenn die Voraussetzungen des § 5 Abs. 7 eingehalten werden). Diese Personen führen auch sonstige notwendige Bedienungen durch (z. B. Behebung technischer Störungen) bzw. sind anwesend, während ein Dritter unter Einhaltung der Voraussetzungen des § 5 Abs. 8 diese durchführt. Der Datenschutzbeauftragte hat stets ein Kontrollrecht.

4. Die Videoüberwachungsanlage ist in einem mittels Schloss besonders geschützten Raum zu betreiben, so dass er nur von [den Mitarbeitern der Abteilung ...] betreten werden kann. Der Zugang zur Videoüberwachungsanlage ist ausschließlich auf dem Administrationsserver des Kamerasystems zu ermöglichen. Dieser ist in einem Schrank zu betreiben, der durch zwei getrennte Schlösser zu sichern ist und zu dem nur die berechtigten Personen Zugang haben. Ein Schlüssel ist durch den Arbeitgeber aufzubewahren, der andere durch den Datenschutzbeauftragten [ODER: den Betriebsrat].

5. Bei Videoüberwachungsanlagen mit Echtzeitübertragung auf Monitore sind die Bilder ausschließlich in die in Anlage 2 festgelegten Räume zu übertragen, zu denen nur die dort namentlich genannten Personen Zutritt haben.

§ 5 Besondere Regelungen für aufzeichnende Systeme

1. Sollen die Videoüberwachungsanlagen die Aufnahmen nicht nur anzeigen, sondern auch speichern und verarbeiten, gelten zusätzlich die Regelungen dieser Bestimmung. Die Speicherung und Verarbeitung von Aufnahmen ist nur zulässig im Rahmen des in § 1 genannten Geltungsbereichs.

2. Als Aufzeichnungssystem ist ein gesondert betriebenes digitales System zu verwenden, das entsprechend den Regelungen des § 4 gegen unrechtmäßigen Zugriff gesichert ist. Die Aufzeichnungen sind auf dem zentralen Administrationsserver der Videoüberwachungsanlage zu speichern und nach Stand der Technik zu verschlüsseln.

3. Aufnahmen von Außenbereichen (§ 2 Abs. 5) sind 72 Stunden nach ihrer Herstellung automatisiert zu löschen. Der Betrieb hat mittels einer „Black Box“ zu erfolgen, in der die Aufnahmen durch einen Ringspeicher nach 72 Stunden automatisiert überschrieben werden. Aufnahmen von Innenbereichen (§ 2 Abs. 3 und 4) sind unverzüglich nach ihrer Auswertung, jedoch spätestens [60] Tage nach

ihrer Herstellung automatisiert zu löschen. Eine längere Speicherung ist nur zulässig, wenn die Daten aufgrund eines konkreten Vorkommnisses im Rahmen des Zwecks der Anlage 1 zur Beweissicherung benötigt werden. Werden Daten länger aufbewahrt, ist regelmäßig zu prüfen, ob die Voraussetzungen der Speicherung weiter vorliegen. Die Löschung hat unverzüglich zu erfolgen, sobald die Daten zur Zweckerreichung nicht mehr notwendig sind. Bei Videoüberwachungsanlagen mit Echtzeitübertragung auf Monitore kann eine Speicherung von Bildern durch die Überwachungsperson manuell ausgelöst und beendet werden, wenn sie dies in Anwendung pflichtgemäßen Ermessens zum Ziele der Zweckerreichung nach Anlage 1 für erforderlich hält und unverzüglich [den Datenschutzbeauftragten und den Betriebsrat] informiert.

4. Soweit es für die Beweissicherung oder Beweisverwertung erforderlich ist, können beweiserhebliche Aufnahmen auf einem anderen Datenträger (z. B. externe Festplatte, Magnetband, USB-Stick) gespeichert werden. Der Schutz des Datenträgers gegen unbefugten Zugriff und die Verschlüsselung nach jeweiligem Stand der Technik muss gewährleistet sein. Die Aufnahmen auf anderen Datenträgern sind, sobald sie nicht mehr zur Beweissicherung benötigt werden, unverzüglich vollständig zu löschen, wenn eine längere Aufbewahrungsdauer nicht gesetzlich vorgeschrieben ist. Soweit die Daten über die genannte Speicherdauer hinaus gespeichert werden, sind diese gem. Art. 18 Abs. 1 DS-GVO in der Verarbeitung zu beschränken und unverzüglich zu löschen, nachdem der Zweck der Speicherung weggefallen ist.

5. Eine Auswertung der Aufnahmen durch visuelle Sichtung via Bildschirm darf nur für die in Anlage 1 festgelegten Zwecke durch die zuvor in Anlage 2 festgelegten, qualifizierten Personen erfolgen. Eine zweckändernde Nutzung ist ausgeschlossen. Die Auswertungen sind nur im Beisein des betrieblichen Datenschutzbeauftragten [und eines Betriebsratsmitglieds] zulässig. Für jede Auswertung ist ein Protokoll gemäß Anlage 3 zu erstellen, in dem Zeitpunkt, Anlass und Ergebnis von den auswertenden Personen niedergeschrieben werden. Die Protokolle sind mit den weiteren Anlagen aufzubewahren.

6. Eine Herausgabe der gespeicherten Aufnahmen an staatliche Stellen ist nur nach einer entsprechenden Anordnung der Staatsanwaltschaft oder einer richterlichen Entscheidung zulässig. Übergabe und Rücknahme der Aufnahmen sind

revisionssicher zu protokollieren. Ein Vertreter von Strafverfolgungsbehörden oder staatlichen Gerichten (Polizei, Staatsanwaltschaft, Richter) kann bei der internen Auswertung anwesend sein.

7. [ENTWEDER:] Eine Übermittlung der gespeicherten Aufnahmen an private Dritte (z. B. Sicherheitsunternehmen) ist nur in Einzelfällen statthaft, wenn die Weitergabe zu deren Aufgabenerfüllung notwendig ist und ein Auftragsverarbeitungsvertrag sowie eine Geheimhaltungsvereinbarung abgeschlossen wurden, die auch die technisch-organisatorische Datensicherheit angemessen berücksichtigen. Vor Übermittlung der Daten an Dritte ist der entsprechende Teil des Formblatts der Anlage 1 auszufüllen. Übergabe und Rücknahme sind revisionssicher zu protokollieren. [ODER:] Eine Übermittlung der gespeicherten Aufnahmen an private Dritte ist unstatthaft.

8. Vor Durchführung von Wartungen oder anderen Eingriffen in das System ist [der Datenschutzbeauftragte/der Betriebsrat] in Textform zu unterrichten. [ENTWEDER:] Wenn ein externer Anbieter Wartungsdienstleistungen durchführt, ist gesondert eine Geheimhaltungsvereinbarung abzuschließen. [ODER:] Es erfolgt keine Fernwartung der Kamerasysteme.

§ 6 Information der Beschäftigten über die Videoüberwachung

1. Eine eingerichtete Videoüberwachung ist den betroffenen Personen stets erkennbar zu machen. Es muss immer ersichtlich sein, welche Videokamera jeweils aktiviert ist.

2. Die Kenntlichmachung erfolgt weiterhin durch ein gut sichtbares Hinweisschild, das so angebracht sein muss, dass es vor Eintritt der betroffenen Person in den Radius der Videoüberwachung sichtbar ist. [Es wird nur das standardisierte Hinweisschild mit folgendem Aussehen eingesetzt: [DIN 33450].] Das Hinweisschild hat zusätzlich den Namen des für die Videoüberwachung Verantwortlichen, dessen Kontaktdaten zur Einholung von Auskünften über die Überwachungskamera sowie einen Link auf die ausführliche Datenschutzerklärung zu enthalten.

3. Spätestens [einen Monat] vor erstmaliger Inbetriebnahme der Videoüberwachung sind die Beschäftigten über die vorliegende Richtlinie durch eine interne E-Mail zu informieren. Neu eingestellten Mitarbeitern ist die Information spätestens zu

Beginn des Arbeitsverhältnisses zu erteilen. Darüber hinaus wird im Eingangsbereich ein deutlich lesbarer Lageplan mit sämtlichen Kameras (Innen- und Außenbereich) sowie der erfassten Bereiche angebracht.

4. Die Einhaltung der Betroffenenrechte nach Art. 15 bis 21 DS-GVO wird sichergestellt.

§ 7 Einbindung des Datenschutzbeauftragten

1. Vor Einrichtung der Videoüberwachung ist eine Datenschutz-Folgenabschätzung nach Art. 35 f. DS-GVO durch die Geschäftsleitung mit Unterstützung des betrieblichen Datenschutzbeauftragten [Kontaktdaten] durchzuführen. Die Durchführung und das Ergebnis der Datenschutz-Folgenabschätzung sind zu dokumentieren und gemeinsam mit den weiteren Prüfunterlagen aufzubewahren.

2. Der Datenschutzbeauftragte ist frühzeitig über die Einrichtung der Videoüberwachung zu informieren. Er ist in die Erstellung des Überwachungsplanes und der Anlagen 1 und 2 einzubeziehen. Ihm sind alle für die Ausübung seiner Kontrollfunktion notwendigen Dokumente und Informationen zur Verfügung zu stellen. Bei geplanten Änderungen an der Videoüberwachung ist der Datenschutzbeauftragte möglichst frühzeitig zu informieren. Seine Stellungnahmen sind zu dokumentieren und gemeinsam mit den weiteren Prüfunterlagen aufzubewahren.

3. Die Videoüberwachung ist in das Verzeichnis von Verarbeitungstätigkeiten aufzunehmen.

§ 8 Einbindung des Betriebsrats

1. Der Betriebsrat hat das Recht zur Beteiligung an der Einrichtung der Videoüberwachungsanlage mit einem seiner Mitglieder und zur Überwachung der Einhaltung der Voraussetzungen dieser Betriebsvereinbarung. Er hat dazu ein Zutrittsrecht zu den Anlagen und Räumen und ein Recht zur Einsichtnahme in sämtliche relevanten Unterlagen.

2. Änderungen des Überwachungssystems sind dem Betriebsrat rechtzeitig vorher mitzuteilen und mit ihm zu beraten. Sie sind nur mit Zustimmung des Betriebsrates zulässig. Erforderlichenfalls entscheidet die Einigungsstelle. Dies gilt auch für alle

anderen Streitigkeiten zwischen [Unternehmen] und dem Betriebsrat aus dieser oder über diese Betriebsvereinbarung.

§ 9 Schlussbestimmungen der Betriebsvereinbarung

1. Die vorliegende Betriebsvereinbarung tritt mit Unterzeichnung in Kraft. [Sie ersetzt sämtliche übrigen Betriebsvereinbarungen zu demselben Themenkreis, insbesondere die Betriebsvereinbarung [Bezeichnung] vom [Datum].]
2. Die Betriebsvereinbarung kann mit einer Frist von [sechs] Monaten zum Ende eines [Kalenderjahres] gekündigt werden [, frühestens jedoch zum [Datum]].
3. Für den Fall der Kündigung dieser Betriebsvereinbarung wirkt sie nach, bis sie durch eine andere Abmachung ersetzt wird.]]

Anlagen:

[Datum, Unterschriften] [Datum, Unterschriften]

Abbildung 31: Muster Vorlage Betriebsvereinbarung[1245]

1245 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht.

X. Muster-Vorlage
Datenschutzinformationen im Bewerbungsprozess

Information zum Datenschutz über die Verarbeitung von Bewerberdaten nach Art. 13, 14 und 21 der Datenschutz-Grundverordnung (DS-GVO).

[Firma]

[Förmliche Anrede]

Informationen über die Grundlage sowie Vorgaben der Datenschutz-Grundverordnung (Art. 13, 14, 21 DS-GVO). Hinweis auf die Verarbeitung personenbezogener Daten. Hinweis auf die Betroffenenrechte.

1. VERANTWORTLICHE STELLE IM SINNE DES DATENSCHUTZRECHTS

[Firmierung]

[Straße und Hausnummer] [PLZ Ort]

[Telefonnummer] [E-Mail-Adresse] [URL]

2. KONTAKTDATEN (des zuständigen) DATENSCHUTZBEAUFTRAGTEN

[Kontaktdaten des Datenschutzbeauftragten]

[Straße und Hausnummer] [PLZ Ort]

[Telefonnummer] [E-Mail-Adresse] [URL]

3. ZWECKE UND RECHTSGRUNDLAGEN DER VERARBEITUNG

Verarbeitung personenbezogenen Daten im Einklang mit den Bestimmungen der europäischen Datenschutz-Grundverordnung (EU-DS-GVO) und dem Bundesdatenschutzgesetz (BDSG), soweit dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses mit uns erforderlich ist. Rechtsgrundlage ist dabei Art. 88 DS-GVO i. V. m. § 26 BDSG sowie ggf. Art. 6 Abs. 1 lit. b DS-GVO zur Anbahnung oder Durchführung von Vertragsverhältnissen.

Verarbeitung personenbezogener Daten, sofern diese zur Erfüllung rechtlicher Verpflichtungen (Art. 6 Abs. 1 lit. c DS-GVO) oder zur Abwehr von geltend gemachten Rechtsansprüchen gegen [Firma] erforderlich ist. Rechtsgrundlage ist dabei Art. 6 Abs. 1 lit. f DS-GVO.

Das berechtigte Interesse ist beispielsweise eine Beweispflicht in einem Verfahren nach dem Allgemeinen Gleichbehandlungsgesetz (AGG). Erteilung einer ausdrücklichen Einwilligung zur Verarbeitung von personenbezogenen Daten für bestimmte Zwecke, ist die Rechtmäßigkeit dieser Verarbeitung auf Basis Ihrer Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO gegeben.

Eine erteilte Einwilligung kann jederzeit, mit Wirkung für die Zukunft, widerrufen werden (s. Ziffer 9) Kommt es zu einem Beschäftigungsverhältnis zwischen Ihnen und uns, können wir gemäß Art. 88 DS-GVO i. V. m. § 26 BDSG-neu die bereits von Ihnen erhaltenen personenbezogenen Daten für Zwecke des Beschäftigungsverhältnisses weiterverarbeiten, soweit dies für die Durchführung oder Beendigung des Beschäftigungsverhältnisses oder zur Ausübung bzw. Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

4. KATEGORIEN PERSONENBEZOGENER DATEN

[Verarbeitung von] Daten, die im Zusammenhang mit Ihrer Bewerbung stehen. Dies können allgemeine Daten zu Ihrer Person (Name, Anschrift, Kontaktdaten etc.), Angaben zu Ihrer beruflichen Qualifikation und Schulausbildung, Angaben zur beruflichen Weiterbildung sowie ggf. weitere Daten sein, die Sie uns im Zusammenhang mit Ihrer Bewerbung übermitteln.

5. QUELLEN DER DATEN

[Verarbeitung] personenbezogene Daten, die im Rahmen der Kontaktaufnahme bzw. Ihrer Bewerbung von Ihnen postalisch oder per E-Mail erhalten bzw. die Sie uns über [Quellen] übermitteln.

6. EMPFÄNGER DER DATEN

[Weitergabe] personenbezogenen Daten innerhalb [Unternehmen / Firma] ausschließlich an die Bereiche und Personen weiter, die diese Daten zur Erfüllung der vertraglichen und gesetzlichen Pflichten bzw. zur Umsetzung unseres berechtigten Interesses benötigen. Wir können Ihre personenbezogenen Daten an mit uns verbundene Unternehmen übermitteln, soweit dies im Rahmen, der unter Ziffer 3 dieses Datenschutzinformationsblatts dargelegten Zwecke und Rechtsgrundlagen zulässig ist.

Ihre personenbezogenen Daten werden in unserem Auftrag auf Basis von Auftragsverarbeitungsverträgen nach Art. 28 DS-GVO verarbeitet. In diesen Fällen stellen wir sicher, dass die Verarbeitung von personenbezogenen Daten im Einklang mit den Bestimmungen der DS-GVO erfolgt. Die Kategorien von Empfängern sind in diesem Fall Anbieter von Internetdienstanbieter sowie Anbieter von Bewerbermanagementsystemen und -software.

Eine Datenweitergabe an Empfänger außerhalb des Unternehmens erfolgt ansonsten nur, soweit gesetzliche Bestimmungen dies erlauben oder gebieten, die Weitergabe zur Erfüllung rechtlicher Verpflichtungen erforderlich ist oder uns Ihre Einwilligung vorliegt.

7. ÜBERMITTLUNG IN EIN DRITTLAND

Eine Übermittlung in ein Drittland ist nicht vorgesehen.

8. DAUER DER DATENSPEICHERUNG

[Speicherung] personenbezogenen Daten solange diese für die Entscheidung über Ihre Bewerbung erforderlich sind. Ihre personenbezogenen Daten bzw. Bewerbungsunterlagen werden [in der Regel] maximal zwei Monate nach Beendigung des Bewerbungsverfahrens (z. B. der Bekanntgabe der Absageentscheidung) gelöscht, sofern nicht eine längere Speicherung rechtlich erforderlich oder zulässig ist. [Speicherung] personenbezogenen Daten darüber hinaus nur, soweit dies gesetzlich oder im konkreten Fall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen für die Dauer eines Rechtsstreits erforderlich ist. Für den Fall, dass Sie einer längeren Speicherung Ihrer personenbezogenen Daten zugestimmt haben, speichern wir diese nach Maßgabe Ihrer Einwilligungserklärung. Kommt es im Anschluss an das Bewerbungs-verfahren zu einem Beschäftigungsverhältnis, Ausbildungsverhältnis oder Praktikanten-verhältnis, werden Ihre Daten, soweit erforderlich und zulässig, zunächst weiterhin gespeichert und anschließend in die Personalakte überführt. [Entsprechend der Qualifikation] Aufnahme in eine Bewerberdatenbank, um die Möglichkeit offen zu halten, die Bewerber bei künftigen adäquaten Vakanzen bei der Bewerberauswahl zu berücksichtigen. Liegt uns eine entsprechende Einwilligung Ihrerseits vor, werden wir Ihre Bewerbungsdaten nach Maßgabe Ihrer Einwilligung bzw. ggf. zukünftigen Einwilligungen in [Datenbank] speichern.

9. IHRE RECHTE

Jede betroffene Person hat das Recht auf Auskunft nach Art. 15 DS-GVO, das Recht auf Berichtigung nach Art. 16 DS-GVO, das Recht auf Löschung nach Art. 17 DS-GVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DS-GVO, das Recht auf Mitteilung nach Art. 19 DS-GVO sowie das Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO. Darüber hinaus besteht ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde nach Art. 77 DS-GVO, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt. Das Beschwerderecht besteht unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs. Sofern die Verarbeitung von Daten auf Grundlage Ihrer Einwilligung erfolgt, sind Sie nach Art. 7 DS-GVO berechtigt, die Einwilligung in die Verwendung Ihrer personenbezogenen Daten jederzeit zu widerrufen. Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen. Bitte beachten Sie zudem, dass wir bestimmte Daten für die Erfüllung gesetzlicher Vorgaben ggf. für einen bestimmten Zeitraum aufbewahren müssen

Widerspruchsrecht

Soweit die Verarbeitung Ihrer personenbezogenen Daten nach Art. 6 Abs. 1 lit. f DS-GVO zur Wahrung berechtigter Interessen erfolgt, haben Sie gemäß Art. 21 DS-GVO das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit Widerspruch gegen die Verarbeitung dieser Daten einzulegen. Wir verarbeiten diese personenbezogenen Daten dann nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen. Diese müssen Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung muss der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dienen.

[Hinweis auf Kontaktaufnahme des Datenschutzbeauftragten bei Fragen]

10. ERFORDERLICHKEIT DER BEREITSTELLUNG PERSONENBEZOGENER DATEN

[Bereitstellung] personenbezogener Daten im Rahmen von Bewerbungsprozessen ist weder gesetzlich noch vertraglich vorgeschrieben. Sie sind somit nicht verpflichtet, Angaben zu Ihren personenbezogenen Daten zu machen. Bitte beachten Sie jedoch, dass diese für die Entscheidung über eine Bewerbung bzw. einen Vertragsabschluss in Bezug auf ein Beschäftigungsverhältnis mit uns erforderlich sind. Soweit Sie uns keine personenbezogenen Daten bereitstellen, können wir keine Entscheidung zur Begründung eines Beschäftigungsverhältnisses treffen. Wir empfehlen, im Rahmen Ihrer Bewerbung nur solche personenbezogenen Daten anzugeben, die zur Durchführung der Bewerbung erforderlich sind.

11. AUTOMATISIERTE ENTSCHEIDUNGSFINDUNG

Da die Entscheidung über Ihre Bewerbung nicht ausschließlich auf einer automatisierten Verarbeitung beruht, findet keine automatisierte Entscheidung im Einzelfall im Sinne des Art. 22 DS-GVO statt.

Ort, Datum

Datenschutzbeauftragter

Abbildung 32: Muster Datenschutzinformation für Bewerber[1246]

1246 *Ingelheim, Alexander, Fircks, Isabelle, Fünkner, Dominik*, VORLAGE DATENSCHUTZINFORMATIONEN FÜR BEWERBER, https://www.datenschutzexperte.de/fileadmin/user_upload/PDFs/Datenschutzinformation-Muster-Bewerber.pdf.

XI. Muster-Vorlage Einsatz von Social-Media-Plug-Ins:[1247]

Einsatz von Social-Media-Plug-ins

(1) Wir setzen derzeit folgende Social-Media-Plug-Ins ein: [Facebook, Google+, Twitter, Xing, T3N, LinkedIn, Flattr]. Wir nutzen dabei die sog. Zwei-Klick-Lösung. Das heißt, wenn Sie unsere Seite besuchen, werden zunächst grundsätzlich keine personenbezogenen Daten an die Anbieter der Plug-Ins weitergegeben. Den Anbieter des Plug-Ins erkennen Sie über die Markierung auf dem Kasten über seinen Anfangsbuchstaben oder das Logo. Wir eröffnen Ihnen die Möglichkeit, über den Button direkt mit dem Anbieter des Plug-Ins zu kommunizieren. Nur wenn Sie auf das markierte Feld klicken und es dadurch aktivieren, erhält der Plug-In-Anbieter die Information, dass Sie die entsprechende Website unseres Online-Angebots aufgerufen haben. Zudem werden die unter § 3 dieser Erklärung genannten Daten übermittelt. Im Fall von Facebook und Xing wird nach Angaben der jeweiligen Anbieter in Deutschland die IP-Adresse sofort nach Erhebung anonymisiert. Durch die Aktivierung des Plug-Ins werden also personenbezogene Daten von Ihnen an den jeweiligen Plug-In-Anbieter übermittelt und dort (bei US-amerikanischen Anbietern in den USA) gespeichert. Da der Plug-In-Anbieter die Datenerhebung insbesondere über Cookies vornimmt, empfehlen wir Ihnen, vor dem Klick auf den ausgegrauten Kasten über die Sicherheitseinstellungen Ihres Browsers alle Cookies zu löschen.

(2) Wir haben weder Einfluss auf die erhobenen Daten und Datenverarbeitungsvorgänge, noch sind uns der volle Umfang der Datenerhebung, die Zwecke der Verarbeitung, die Speicherfristen bekannt. Auch zur Löschung der erhobenen Daten durch den Plug-In-Anbieter liegen uns keine Informationen vor.

(3) Der Plug-In-Anbieter speichert die über Sie erhobenen Daten als Nutzungsprofile und nutzt diese für Zwecke der Werbung, Marktforschung und/oder bedarfsgerechten Gestaltung seiner Website. Eine solche Auswertung erfolgt insbesondere (auch für nicht eingeloggte Nutzer) zur Darstellung von bedarfsgerechter Werbung und um

1247 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, Lachenmann, S. 558 - 561, Mustervorlage.

andere Nutzer des sozialen Netzwerks über Ihre Aktivitäten auf unserer Website zu informieren. Ihnen steht ein Widerspruchsrecht gegen die Bildung dieser Nutzerprofile zu, wobei Sie sich zur Ausübung dessen an den jeweiligen Plug-In-Anbieter wenden müssen. Über die Plug-Ins bieten wir Ihnen die Möglichkeit, mit den sozialen Netzwerken und anderen Nutzern zu interagieren, so dass wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten können. Rechtsgrundlage für die Nutzung der Plug-Ins ist Art. 6 Abs. 1 S. 1 lit. f DS-GVO.

(4) Die Datenweitergabe erfolgt unabhängig davon, ob Sie ein Konto bei dem Plug-In-Anbieter besitzen und dort eingeloggt sind. Wenn Sie bei dem Plug-In-Anbieter eingeloggt sind, werden Ihre bei uns erhobenen Daten direkt Ihrem beim Plug-In-Anbieter bestehenden Konto zugeordnet. Wenn Sie den aktivierten Button betätigen und z. B. die Seite verlinken, speichert der Plug-In-Anbieter auch diese Information in Ihrem Nutzerkonto und teilt sie Ihren Kontakten öffentlich mit. Wir empfehlen Ihnen, sich nach Nutzung eines sozialen Netzwerks regelmäßig auszuloggen, insbesondere jedoch vor Aktivierung des Buttons, da Sie so eine Zuordnung zu Ihrem Profil bei dem Plug-In-Anbieter vermeiden können.

(5) Weitere Informationen zu Zweck und Umfang der Datenerhebung und ihrer Verarbeitung durch den Plug-In-Anbieter erhalten Sie in den im Folgenden mitgeteilten Datenschutzerklärungen dieser Anbieter. Dort erhalten Sie auch weitere Informationen zu Ihren diesbezüglichen Rechten und Einstellungsmöglichkeiten zum Schutze Ihrer Privatsphäre.

(6) Adressen der jeweiligen Plug-In-Anbieter und URL mit deren Datenschutzhinweisen:

a. [Facebook Inc., 1601 S California Ave, Palo Alto, California 94304, USA; http://www.facebook.com/policy.php; weitere Informationen zur Datenerhebung: http://www.facebook.com/help/186325668085084, http://www.facebook.com/about/privacy/your-info-on-other#applications sowie http://www.facebook.com/about/privacy/your-info#everyoneinfo. Facebook hat sich dem EU-US-Privacy-Shield unterworfen, https://www.privacyshield.gov/EU-US-Framework.

b. Google Inc., 1600 Amphitheater Parkway, Mountainview, California 94043, USA; https://www.google.com/policies/privacy/partners/?hl=de. Google hat sich dem EU-US-Privacy-Shield unterworfen, https://www.privacyshield.gov/EU-US-Framework.

c. Twitter, Inc., 1355 Market St, Suite 900, San Francisco, California 94103, USA; https://twitter.com/privacy. Twitter hat sich dem EU-US-Privacy-Shield unterworfen, https://www.privacyshield.gov/EU-US-Framework.

d. Xing AG, Gänsemarkt 43, 20354 Hamburg, DE; http://www.xing.com/privacy.

e. T3N, yeebase media GmbH, Kriegerstr. 40, 30161 Hannover, Deutschland; https://t3n.de/store/page/datenschutz.

f. LinkedIn Corporation, 2029 Stierlin Court, Mountain View, California 94043, USA; http://www.linkedin.com/legal/privacy-policy. LinkedIn hat sich dem EU-US-Privacy-Shield unterworfen, https://www.privacyshield.gov/EU-US-Framework.

g. Flattr Network Ltd. mit Sitz in 2 nd Floor, White bear yard 114A, Clerkenwell Road, London, Middlesex, England, EC1R 5DF, Großbritannien; https://flattr.com/privacy.]

I. AddThis-Bookmarking

(1) Unsere Webseiten enthalten zudem AddThis-Plug-Ins. Diese Plug-Ins ermöglichen Ihnen das Setzen von Bookmarks bzw. das Teilen von interessanten Inhalten mit anderen Nutzern. Über die Plug-Ins bieten wir Ihnen die Möglichkeit, mit den sozialen Netzwerken und anderen Nutzern zu interagieren, so dass wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten können. Rechtsgrundlage für die Nutzung der Plug-Ins ist Art. 6 Abs. 1 S. 1 lit. f DS-GVO.

(2) Über diese Plug-Ins baut Ihr Internetbrowser eine direkte Verbindung mit den Servern von AddThis und gegebenenfalls dem gewählten sozialen Netzwerk- oder Bookmarking-Dienst auf. Die Empfänger erhalten die Information, dass Sie die entsprechende Website unseres Online-Angebots aufgerufen haben und die unter § 3 dieser Erklärung genannten Daten. Diese Informationen werden auf den Servern von AddThis in den USA verarbeitet. [Wir haben Standarddatenschutzklauseln mit AddThis abgeschlossen.]. Wenn Sie Inhalte auf unserer Webseite an soziale Netzwerke oder Bookmarking-Dienste senden, kann eine Verbindung zwischen dem Besuch unserer Webseite und Ihrem Nutzerprofil bei dem entsprechenden Netzwerk hergestellt werden. Wir haben weder Einfluss auf die erhobenen Daten und Datenverarbeitungsvorgänge, noch sind uns der volle Umfang der Datenerhebung, die

Zwecke der Verarbeitung, die Speicherfristen bekannt. Auch zur Löschung der erhobenen Daten durch den Plug-in-Anbieter liegen uns keine Informationen vor.

(3) Der Plug-in-Anbieter speichert diese Daten als Nutzungsprofile und nutzt diese für Zwecke der Werbung, Marktforschung und/oder bedarfsgerechten Gestaltung seiner Website. Eine solche Auswertung erfolgt insbesondere (selbst für nicht eingeloggte Nutzer) zur Erbringung von bedarfsgerechter Werbung und um andere Nutzer des sozialen Netzwerks über Ihre Aktivitäten auf unserer Website zu informieren. Ihnen steht ein Widerspruchsrecht zu gegen die Bildung dieser Nutzerprofile, wobei Sie sich zur Ausübung dessen an den jeweiligen Plug-In-Anbieter richten müssen.

(4) Wenn Sie nicht an diesem Verfahren teilnehmen möchten, können Sie der Datenerhebung und -speicherung jederzeit durch Setzen eines Opt-out-Cookies mit Wirkung für die Zukunft widersprechen: http://www.addthis.com/privacy/opt-out. Alternativ können Sie Ihren Browser so einstellen, dass er das Setzen eines Cookies verhindert.

(5) Weitere Informationen zu Zweck und Umfang der Datenerhebung und ihrer Verarbeitung durch den Plug-In-Anbieter sowie weitere Informationen zu Ihren diesbezüglichen Rechten und Einstellungsmöglichkeiten zum Schutze Ihrer Privatsphäre erhalten Sie bei: AddThis LLC, 1595 Spring Hill Road, Sweet 300, Vienna, VA 22182, USA, www.addthis.com/privacy.

II. Einbindung von YouTube-Videos

(1) Wir haben YouTube-Videos in unser Online-Angebot eingebunden, die auf http://www.YouTube.com gespeichert sind und von unserer Website aus direkt abspielbar sind. [Diese sind alle im „erweiterten Datenschutz-Modus“ eingebunden, d. h., dass keine Daten über Sie als Nutzer an YouTube übertragen werden, wenn Sie die Videos nicht abspielen. Erst wenn Sie die Videos abspielen, werden die in Absatz 2 genannten Daten übertragen. Auf diese Datenübertragung haben wir keinen Einfluss.]

(2) Durch den Besuch auf der Website erhält YouTube die Information, dass Sie die entsprechende Unterseite unserer Website aufgerufen haben. Zudem werden die unter § 3 dieser Erklärung genannten Daten übermittelt. Dies erfolgt unabhängig davon, ob YouTube ein Nutzerkonto bereitstellt, über das Sie eingeloggt sind, oder ob kein Nutzerkonto besteht. Wenn Sie bei Google eingeloggt sind, werden Ihre Daten direkt Ihrem Konto zugeordnet. Wenn Sie die Zuordnung mit Ihrem Profil bei YouTube nicht wünschen, müssen Sie sich vor Aktivierung des Buttons ausloggen. YouTube speichert Ihre Daten als Nutzungsprofile und nutzt sie für Zwecke der Werbung, Marktforschung

und/oder bedarfsgerechten Gestaltung seiner Website. Eine solche Auswertung erfolgt insbesondere (selbst für nicht eingeloggte Nutzer) zur Erbringung von bedarfsgerechter Werbung und um andere Nutzer des sozialen Netzwerks über Ihre Aktivitäten auf unserer Website zu informieren. Ihnen steht ein Widerspruchsrecht zu gegen die Bildung dieser Nutzerprofile, wobei Sie sich zur Ausübung dessen an YouTube richten müssen.

(3) Weitere Informationen zu Zweck und Umfang der Datenerhebung und ihrer Verarbeitung durch YouTube erhalten Sie in der Datenschutzerklärung. Dort erhalten Sie auch weitere Informationen zu Ihren Rechten und Einstellungsmöglichkeiten zum Schutze Ihrer Privatsphäre: https://www.google.de/intl/de/policies/privacy. Google verarbeitet Ihre personenbezogenen Daten auch in den USA und hat sich dem EU-US-Privacy-Shield unterworfen, https://www.privacyshield.gov/EU-US-Framework.

III. Einbindung von Google Maps

(1) Auf dieser Webseite nutzen wir das Angebot von Google Maps. Dadurch können wir Ihnen interaktive Karten direkt in der Website anzeigen und ermöglichen Ihnen die komfortable Nutzung der Karten-Funktion.

(2) Durch den Besuch auf der Website erhält Google die Information, dass Sie die entsprechende Unterseite unserer Website aufgerufen haben. Zudem werden die unter § 3 dieser Erklärung genannten Daten übermittelt. Dies erfolgt unabhängig davon, ob Google ein Nutzerkonto bereitstellt, über das Sie eingeloggt sind, oder ob kein Nutzerkonto besteht. Wenn Sie bei Google eingeloggt sind, werden Ihre Daten direkt Ihrem Konto zugeordnet. Wenn Sie die Zuordnung mit Ihrem Profil bei Google nicht wünschen, müssen Sie sich vor Aktivierung des Buttons ausloggen. Google speichert Ihre Daten als Nutzungsprofile und nutzt sie für Zwecke der Werbung, Marktforschung und/oder bedarfsgerechten Gestaltung seiner Website. Eine solche Auswertung erfolgt ins-besondere (selbst für nicht eingeloggte Nutzer) zur Erbringung von bedarfsgerechter Werbung und um andere Nutzer des sozialen Netzwerks über Ihre Aktivitäten auf unserer Website zu informieren. Ihnen steht ein Widerspruchsrecht zu gegen die Bildung dieser Nutzerprofile, wobei Sie sich zur Ausübung dessen an Google richten müssen.

(3) Weitere Informationen zu Zweck und Umfang der Datenerhebung und ihrer Verarbeitung durch den Plug-in-Anbieter erhalten Sie in den Datenschutzerklärungen des Anbieters. Dort erhalten Sie auch weitere Informationen zu Ihren diesbezüglichen

Rechten und Einstellungsmöglichkeiten zum Schutze Ihrer Privatsphäre: http://www.google.de/intl/de/policies/privacy. Google verarbeitet Ihre personenbezogenen Daten auch in den USA und hat sich dem EU-US Privacy Shield unterworfen, https://www.privacyshield.gov/EU-US-Framework.[1248]

1248 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, Lachenmann, S. 558–561, Mustervorlage.

XII. Muster Einwilligungserklärung zur Speicherung von Bewerberdaten

Einwilligungserklärung zur Speicherung von Bewerberdaten

Sollte meine Bewerbung nicht erfolgreich sein, willige ich ein, dass [potenzieller Arbeitgeber] meine personenbezogenen Daten, die ich im Rahmen des gesamten Bewerbungsverfahrens mitgeteilt habe (zum Beispiel in Anschreiben, Lebenslauf, Zeugnissen, Bewerber-Fragebögen, Bewerber-Interviews,), über das Ende des konkreten Bewerbungsverfahrens hinaus speichert. Ich willige ein, dass [potenzieller Arbeitgeber] diese Daten nutzt, um mich später zu kontaktieren und das Bewerbungsverfahren fortzusetzen, falls ich für eine andere Stelle in Betracht kommen sollte.

[Optional: Sofern ich in meinem Bewerbungsschreiben oder anderen von mir im Bewerbungsverfahren eingereichten Unterlagen selbst „besondere Kategorien personenbezogener Daten“ nach Art. 9 der Datenschutz-Grundverordnung mitgeteilt habe (z.B. ein Foto, das die ethnische Herkunft erkennen lässt, Angaben über Schwerbehinderten Eigenschaft, usw.), bezieht sich meine Einwilligung auch auf diese Daten. [Arbeitgeber] möchte allerdings alle Bewerber nur nach ihrer Qualifikation bewerten und bittet daher, auf solche Angaben in der Bewerbung möglichst zu verzichten.]

[Optional:

Diese Einwilligung gilt zudem für Daten über meine Qualifikationen und Tätigkeiten aus allgemein zugänglichen Datenquellen (insbesondere berufliche soziale Netzwerke), die [Arbeitgeber] im Rahmen des Bewerbungsverfahrens zulässig erhoben hat.] Meine Daten werden nicht an Dritte weitergegeben.

Diese Einwilligung ist freiwillig und hat keine Auswirkungen auf meine Chancen im jetzigen Bewerbungsverfahren. Ich kann sie ohne Angabe von Gründen verweigern, ohne dass ich deswegen Nachteile zu befürchten hätte. Ich kann meine Einwilligung zudem jederzeit [– zum Beispiel online über das Bewerbungssystem –] widerrufen; in diesem Fall werden meine Daten nach Abschluss des Bewerbungsverfahrens unverzüglich gelöscht.

Zusatzerklärung bei besonderen Kategorien von Daten:

Meine Bewerbung bei [Arbeitgeber] enthält besondere Kategorien personenbezogener Daten (z. B. Angaben zum Familienstand, die Informationen über mein Sexualleben oder meine sexuelle Orientierung geben können; Angaben zu meiner Gesundheit; ein Foto, das Rückschlüsse auf meine ethnische Herkunft und ggf. meine Sehkraft und/oder Religion erlaubt; ähnlich sensible Daten im Sinne von Artikel 9 der Datenschutz-Grundverordnung). Meine Bewerbung darf daher in der vorliegenden Form nur mit meiner Einwilligung verarbeitet werden. Ich willige ein, dass [Arbeitgeber] die besonderen Kategorien personenbezogener Daten, die in meinem Bewerbungsschreiben und den beigefügten Unterlagen enthalten sind, zum Zweck der Durchführung des Bewerbungs-verfahrens verarbeitet. Diese Einwilligung dient ausschließlich dazu, die Bewerbung in ihrer vorliegenden Form überhaupt berücksichtigen zu können. Die Informationen werden keine Berücksichtigung im Bewerbungsprozess finden, soweit nicht – insbesondere bei Schwerbehinderten – eine gesetzliche Verpflichtung hierfür besteht.

Meine Daten werden nicht an Dritte weitergegeben. Ich bin nicht verpflichtet, diese Einwilligung zu erteilen und kann stattdessen eine um die besonderen Kategorien personenbezogener Daten bereinigte Bewerbung einreichen, ohne dass dies Auswirkungen auf meine Chancen im Bewerbungsverfahren haben. Ich kann meine Einwilligung ohne Angabe von Gründen verweigern und eine erteilte Einwilligung jederzeit widerrufen. Im Fall des Widerrufs werden meine von der Einwilligung umfassten Daten unverzüglich gelöscht. Im Fall der Nichterteilung oder des Widerrufs der Einwilligung kann meine bereits eingereichte Bewerbung allerdings nicht in der vorliegenden Form berücksichtigt werden.

Abbildung 33: Einwilligungserklärung zur Speicherung von Bewerberdaten [1249]

1249 *Koreng u. a.* (Hrsg.), Formularhandbuch Datenschutzrecht, Bergt, S. 810, Abschnitt H. Beschäftigtendatenschutz.

EIKV-Schriftenreihe zum Wissens- und Wertemanagement

Jahr	Autor/ Autorin	Titel	Band
2020	Marcus Bäumer	What matters to investment professionals in decision making? - The role of soft factors in stock selection	44
2020	Murad Erserbetci	Einführung der EU-Datenschutz-Grundverordnung: Auswirkungen und Handlungsempfehlungen für die Unternehmensbereiche, Geschäftsleitung, Personal sowie Informationstechnologie	43
2020	Sarah Holzhauer	Die Umsetzung eines inklusiven Bewerbungs-prozesses für Menschen mit Behinderung	42
2020	Holger Niemitz	Sein oder Nichtsein von Patentboxen in verschiedenen Ländern im Rechtsvergleich des Steuerberaters	41
2020	Maximilien Petit	Management von Freiwilligen in luxemburgischen Non-Profit Organisationen - Einige Empfehlungen für die Praxis	40
2020	Jens Hoellermann	ESG in Private Equity and other alternative asset classes: What the industry has accomplished so far regarding Environmental, Social and Governance matters	39
2020	Ulrike Vizethum	Immaterielle Ressourcen, Basis der Wertschöpfung im Gesundheitswesen. Eine quantitative Analyse, gezeigt am Beispiel einer antimikrobiellen photodynamischen Therapie (aPDT) in der Zahnmedizin.	38
2020	André Reuter	Postgraduale Weiterbildung im Gesundheitswesen, gezeigt am Beispiel der DTMD University mit Beiträgen von Thomas Gergen und Ralf Rössler	37
2020	Ulrich J. Grimm	Nachweis der rechtserhaltenden Benutzung von Marken in einem internationalen Konzern Vergleich der Rechtsvorschriften und Rechtsprechung in Deutschland, der Europäischen Union, den USA sowie im Rahmen der internationalen Registrierung einer Marke (Probleme, Konsequenzen und Lösungsmöglichkeiten)	36
2020	Anne Bartel- Radic, André Reuter (Hg)	Studien zum Strategischen Management und Personalmanagement	35
2020	Diana Pereira Dias	Analyse de la phase transitoire de la loi du 3 février 2018 portant sur le bail commercial au Luxembourg	34
2019	Anne Bartel-Radic (Hg)	Méthodes de recherche innovantes et alternatives en économie et gestion - Innovative and alternative research methods in economics and business administration	33
2019	André Reuter Thomas Gergen (Hg)	Studien zum Wissens- und Wertemanagement Investment, Gesundheitswesen, Non-Profit-Organisationen, Datenschutz und Patentboxen	32

Jahr	Autor/ Autorin	Titel	Band
2018	Alina Bongartz	Der Einfluss der Kundenzufriedenheit auf den Unternehmenserfolg - die Wirkung von Value Added Services	31
2018	Lisa Schreiner	The Effects of Remuneration and Reward Systems on Employee Motivation in Luxembourg	30
2018	Sven Kirchens	TVA - Introduction du mécanisme de l'autoliquidation dans le secteur de la construction au Luxembourg ? Analyse et Propositions	29
2018	Romain Gennen	Die automobile (R)Evolution – das automobile Smartphone	28
2018	Désirée Kaupp	Corporate culture - an underestimated intangible asset for the information society	27
2018	Claudia Lamberti	Women in management and the issue of gender-based barriers - An empirical study of the business sector in Europe	26
2018	Alexander Vollmer	Überwachung von ausgelagerten Funktionen und Kompetenzen in der luxemburgischen Fondsindustrie	25
2017	Nadine Allar	Identification and Measurement of Intangibles in a Knowledge Economy - The special relevance of human capital	24
2017	Johanna Brachmann	Ist das Arbeitnehmererfindungsrecht erneut reformbedürftig? - Ein Rechtsvergleich zwischen Deutschland und Österreich, Schweiz, USA, Großbritannien	23
2017	Christophe Santini	Burn-Out / Bore-Out - Équivalences, similitudes et différences impactant la vie socio-économique des personnes concernées	22
2017	Andrea Dietz	Anti-Money Laundering and Counter- Terrorist Financing in the Luxembourg Investment Fund Market	21
2017	Sebastian Fontaine	Quo vadis Digitalisierung? Von Industrie 4.0 zur Circular-Economy	20
2017	Patrick Matthias Sprenker	RAIF – Reserved Alternative Investment Fund – The impact on the Luxembourg Fund Market and the Alternative Investment Fund landscape	19
2017	Marco Pate	Kriterien zur Kreditbesicherung mit Immaterialgüterrechten anhand der Finanzierungsbesicherung mit Immobilien	18
2016	Niklas Jung	Abolition of the Safe Harbor Agreement – Legal situation and alternatives	17
2016	Daniel Nepgen	Machbarkeitsstudie eines Audioportals für Qualitätsjournalismus. Eine empirische Untersuchung in Luxemburg	16
2016	Alexander Fey	Warum Immaterielle Wirtschaftsgüter und Intellectual Property die Quantenteilchen der Ökonomie sind	15
2016	Stefanie Roth	The Middle Management – new awareness needed in the current information society?	14

Jahr	Autor/ Autorin	Titel	Band
2016	Peter Koster	Luxembourg as an aspiring platform for the aircraft engine industry	13
2016	Julie Wing Yan Chow	Activity Based Costing - A case study of Raiffeisen Bank of Luxembourg	12
2016	Meika Schuster	Ursachen und Folgen von Ausbildungsabbrüchen	11
2016	Nadine Jneidi	Risikofaktor Pflichtteil - Grundlagen und Grenzen der Regelungs- und Gestaltungsmöglichkeiten von Pflichtteilsansprüchen bei der Nachfolge in Personengesellschaften	10
2016	Christian Wolf	Zur Eintragungsfähigkeit von Geruchs- und Hörmarken	9
2016	Torsten Hotop	Äquivalenzinteresse im Erfinderrecht	8
2016	Lars Heyne	Immaterialgüterrechte und Objektreplikation: Juristische Risiken und Lösungsmöglichkeiten bei der Vermarktung von 3D-Druckvorlagen	7
2016	Dr. Sverre Klemp	Die Angemessenheit der Vergütung nach § 32 UrhG für wissenschaftliche Werke im STM-Bereich	6
2016	Irena Hank	Emotionale Intelligenz und optimales Teaming – eine empirische Untersuchung	4
2016	Tim Karius	Intellectual Property and Intangible Assets - Alternative valuation and financing approaches for the knowledge economy in Luxembourg	3
2016	Sebastian Fontaine	The electricity market reinvention by regional renewal	2
2015	Francesca Schmitt	Intellectual Property and Investment Funds	1

Anzeige

University for Digital Technologies in Medicine & Dentistry Luxembourg

Berufsbegleitend zum Doktortitel
Deutschsprachige Doktorandenschule in
Advanced Medicine (DAM) und Business Administration (DBA)
an der DTMD University Luxemburg

Das seit 2004 im Großherzogtum etablierte European Institute for Knowledge and Value Management (EIKV), Herausgeber dieser Schriftenreihe, bündelt in Zusammenarbeit mit der DTMD University for Digital Technologies in Medicine and Dentistry (DTMD) und internationalen universitären Kooperationspartnern die Aktivitäten in Lehre und Forschung des berufsbegleitenden deutschsprachigen DAM/DBA Doktorandenprogramms im Schloss Wiltz in Luxemburg.

Angesprochen sind in erster Linie approbierte Ärztinnen und Ärzte sowie Führungskräfte mit einem anerkannten Master-Hochschulabschluss und mindestens drei bis fünf Jahren Berufserfahrung in eigener Praxis, Klinik, Forschungseinrichtung, Unternehmung oder Verwaltung, die:

- ihre fachlichen, beruflichen und sozialen Kompetenzen in einer hochwertigen wissenschaftlich fundierten und praxisorientierten Promotionsarbeit, der These, dokumentieren möchten, mit der Möglichkeit, diese in der Schriftenreihe des EIKV zu veröffentlichen,
- ihre beruflichen Fähigkeiten und ihre fachliche Expertise durch einen persönlichen, wissenschaftlich abgesicherten Reflexions- und Forschungsprozess aufwerten wollen,
- dabei ihr persönliches Profil und ihre bisherigen beruflichen Leistungen mit einem anerkannten akademischen Titel zur Geltung bringen möchten.

Die DAM/DBA Executive Doctorates in Advanced Medine und Business Administration basieren auf einem von einem internationalen wissenschaftlichen Team an der Harvard University validierten Konzept, das von ausgewiesenen Professoren mit umfangreichen klinischen und praktischen Erfahrungen geleitet werden.

Informationen und Bewerbung
European Institute for Knowledge & Value Management A.s.b.l.
Prof. Dr. Dr. Thomas Gergen
8, rue de la source, L-6998 Hostert, Luxemburg
E-Mail: thomas.gergen@eikv.org