Steinhart, Alexander; Zerres, Thomas; Zerres, Christopher

Working Paper

Rechtskonforme Datenlöschkonzepte

Arbeitspapiere für Marketing und Management, No. 55

Provided in Cooperation with:
Fakultät Medien, Hochschule Offenburg

Suggested Citation: Steinhart, Alexander; Zerres, Thomas; Zerres, Christopher (2021) : Rechtskonforme Datenlöschkonzepte, Arbeitspapiere für Marketing und Management, No. 55, Hochschule Offenburg, Fakultät Medien, Offenburg, https://doi.org/10.48584/opus-4988

This Version is available at:
https://hdl.handle.net/10419/244672

CHRISTOPHER ZERRES

MARKETING

Schriftenreihe „Arbeitspapiere für Marketing und Management“

Herausgeber:
Prof. Dr. Christopher Zerres

Hochschule Offenburg
Fakultät Medien und Informationswesen

Arbeitspapier Nr. 55

Rechtskonforme Datenlöschkonzepte

Ein Wegweiser für die betriebliche Praxis mit einem Fokus auf die Datenauftragsverarbeitung

Steinhart, A., Zerres, T., Zerres, C.

Offenburg, April 2021

ISSN: 2510-4799

Impressum

Prof. Dr. Christopher Zerres
Hochschule Offenburg
Fakultät Medien und Informationswesen
Badstraße 24
77652 Offenburg

ISSN: 2510-4799

Inhalt

1 EINFÜHRUNG

„Datenschutz und Informationsfreiheit sind moderne Grundrechte. Sie garantieren unsere Selbstbestimmung im beginnenden digitalen Zeitalter: Die Freiheit, unsere Daten zu nützen – aber auch die Freiheit, unsere Daten zu schützen!“ – Stefan Brink.[1]

Die mit dem Stichtag 25. Mai 2018 in Kraft getretene Datenschutz-Grundverordnung (DS-GVO) hat zu einem enormen Anstieg der Aufmerksamkeit auf diesem Gebiet, sowohl bei den betroffenen Personen als auch bei den datenverarbeitenden Unternehmen geführt. Gemäß einer Aussage des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Stefan Brink, konnte die Quote der aktiven Umsetzung der datenschutzrechtlichen Vorschriften in den Betrieben von bisher einem Drittel auf zwei Drittel mit positivem Trend angehoben werden. Seitdem die DS-GVO Gültigkeit erlangt hat, werden Umfragen zur praktischen Umsetzung der DS-GVO durchgeführt. Kaum ein Ergebnis einer dieser Umfragen besagt, dass die Umsetzung bei allen Betrieben nahezu abgeschlossen wäre. Der Digitalverband Bitkom hat eine repräsentative Befragung unter 500 Unternehmen in ganz Deutschland durchgeführt. Fast eineinhalb Jahre nach dem Geltungsbeginn der DS-GVO hatten zwar zwei Drittel der Befragten die DS-GVO größtenteils umgesetzt, bei lediglich 25 Prozent war die Umsetzung bereits zum Zeitpunkt der Umfrage vollständig abgeschlossen.[2] Auch daran lässt sich erkennen, dass sich in den ersten zwei Jahren einige Herausforderungen in der betrieblichen Praxis ergeben haben. Zum einen kennen die betroffenen Personen ihre Rechte besser als zuvor und zum anderen haben hohe Bußgelder bei Nichteinhaltung der gesetzlichen Vorschriften eine abschreckende Wirkung. Bisher sind diese zwar meist von erheblichen Bußgeldern und einer Abmahnwelle verschont geblieben, dennoch ist ein konsequentes Vorgehen der Aufsichtsbehörden zu beobachten. An der Verdreifachung des Arbeitsvolumens und der Aufstockung der Datenschutzbereiche sowohl bei den Behörden als auch in den Unternehmen lässt sich die gestiegene Bedeutung dieses Bereichs deutlich erkennen.[3] Die Verarbeitung von personenbezogenen Daten stellt für viele Unternehmen einen äußerst hohen wirtschaftlichen Wert dar. Sie spielen eine derart große Rolle, dass sie bereits als „Währung der Zukunft“[4] bezeichnet werden. Gerade in Zeiten von Big Data und vielen neuen technischen Möglichkeiten im Bereich der Verarbeitung personenbezogener Daten sollen durch die DS-GVO Verbraucherrechte und die Privatsphäre geschützt werden.[5] Die rechtlichen Anforderungen stellen die Unternehmen vor komplexe Aufgaben. Dadurch entsteht eine neue Art der Zusammenarbeit zwischen den Unternehmen, ihren Kunden, Lieferanten und sämtlichen externen Geschäftspartnern.

---

[1] *Brink, Stefan*: „Person des Beauftragten“, URL: https://www.baden-wuerttemberg.datenschutz.de/der-landesbeauftragte-fuer-den-datenschutz-und-die-informationsfreiheit-baden-wuerttemberg, Abruf: 14.09.2020.

[2] Vgl. *Bitkom e.V.*: „DS-GVO, ePrivacy, Brexit – Datenschutz und die Wirtschaft“, URL: https://www.bitkom.org/sites/default/files/2019-09/bitkom-charts-pk-privacy-17-09-2019.pdf, S. 2, Abruf: 16.09.2020.

[3] Vgl. *Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg*: „Tätigkeitsbericht 2018“, URL: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/LfDI-34.-Datenschutz-Tätigkeitsbericht-Internet.pdf, S. 94, Abruf: 14.09.2020.

[4] Vgl. *Martini, Mario,* in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 1. Aufl., C.H. Beck, München 2017, DS-GVO Art. 25 Rn. 45; *Reiners, Wilfried*: Datenschutz in der Personal Data Economy – Eine Chance für Europa, in: Zeitschrift für Datenschutz, 02/2015, S. 55.

[5] Vgl, *Hanschke, Inge*: Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten – Eine kompakte Einführung in die Praxis, 2. Auflage, Springer, Wiesbaden 2020, S. 23.

Insbesondere die Stärkung der Betroffenenrechte und das damit verbundene Recht auf Löschung gemäß Art. 17 DS-GVO stellt viele Unternehmen vor Herausforderungen. Täglich wird mit einer Vielzahl von Anwendungssystemen gearbeitet, die personenbezogene Daten verarbeiten und traditionell darauf ausgerichtet sind, diese langfristig und sicher aufzubewahren. In den meisten IT-Entwicklungsprozessen war das Löschen von personenbezogenen Daten trotz der Wichtigkeit bisher kein Thema.[6] Nun werden Prozesse gefordert, die ein möglichst schnelles und endgültiges Löschen ermöglichen, was die Unternehmen häufig auch vor technische Herausforderungen stellt. Es müssen transparente Regeln für die Erfassung, Speicherung, Löschung und Dokumentation dieser Daten festgelegt werden.[7] Erschwerend kommen gesetzliche und mögliche interne Aufbewahrungspflichten sowie Abhängigkeiten zwischen den verschiedenen Systemen hinzu.[8] Insbesondere die globale Aufstellung von Konzernen führt zu der Erfordernis einer gruppenweiten Lösung um den datenschutzrechtlichen Anforderungen gerecht werden zu können. Ein besonderes Hindernis stellen über Jahrzehnte gewachsene Datenbestände dar, bei denen nicht mehr erkennbar ist, zu welchem Zweck sie gespeichert worden sind und ob dieser Zweck bereits erfüllt wurde.[9] Aufgrund der enormen Anzahl an personenbezogenen Daten steht die fristgerechte und rechtskonforme Löschung bei den Aufsichtsbehörden im Fokus.[10] Der Gesetzgeber macht keine Vorgaben zur technischen und organisatorischen Umsetzung, was verschiedene Lösungsansätze zur Folge hat. Je nach Branche, Art, und Größe des Unternehmens unterscheiden sich die Problemstellungen und der Aufwand durchaus deutlich. Zwar stellt etwa das Deutsche Institut für Normung (DIN) mit der DIN 66398 „Leitlinien zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“ zur Verfügung, worin Vorgehensweisen zu unterschiedlichen Datenarten, Löschfristen und Löschregeln beschrieben werden, jedoch bleiben weiterhin offene Fragen und Schwierigkeiten für die Unternehmen. Nicht selten wird der Wunsch nach Konkretisierungen und Spezifizierungen durch den Gesetzgeber geäußert, um den Unsicherheiten in diesem Bereich, sowie im gesamten sekundärrechtlichen Datenschutzrecht entgegenzuwirken.[11] Bei der Implementierung eines Löschkonzepts müssen die Geschäftsprozesse ständig weiterentwickelt und angepasst werden. Nach einer Querschnittsprüfung bei 50 Unternehmen im November 2019 sieht die Landesbeauftragte für den Datenschutz in Niedersachen einen „erheblichen Handlungsbedarf“ in diesem Bereich.[12] Die Thematik hat in der Praxis also eine große Relevanz und dabei stellt sich die Frage nach den exakten betrieblichen Herausforderungen und praktikablen Lösungen für die Unternehmen.

Eine weitere Komplexität bringt die Auftragsverarbeitung gemäß Art. 28 DS-GVO und die damit verbundene Verpflichtung der Auftragsverarbeiter, entsprechende technische und organisatorische Maßnahmen (TOMs) vorhalten zu müssen mit sich. Die Auftragsverarbeitung

[6] Vgl. *Berning, Wilhelm; Keppeler, Lutz Martin*: „Technische und rechtliche Probleme bei der Umsetzung der DS-GVO Löschpflichten“, in: Zeitschrift für Datenschutz, 07/2017, S. 314.
[7] Vgl. *Mühlbauer, Holger*: EU-Datenschutz-Grundverordnung (DSGVO) – Praxiswissen für die Umsetzung im Unternehmen – Schnellübersichten, 2. Auflage, Beuth Verlag, Berlin 2018, S. 1.
[8] Vgl. *Ebert, Nico; Knuchel, Christian*: “DSGVO-konformes Löschen – Ein Praxisbericht zur Umsetzung von Artikel 17 bei der AXA Schweiz AG“, in: Datenschutz und Datensicherheit, 02/2020, S. 126.
[9] Vgl. *Berning, Wilhelm; Keppeler, Lutz Martin*: „Technische und rechtliche Probleme bei der Umsetzung der DS-GVO Löschpflichten“, in: Zeitschrift für Datenschutz, 07/2017, S. 317.
[10] Vgl. *Ingelheim, Alexander*: „Das erste Jahr DSGVO - Eine Bestandsaufnahme“, in: *Controlling & Management Review* 63, 04/2019, S. 69.
[11] Vgl. *Jaspers, Andreas; Jacquemain, Tobias*: „Datenschutz-Grundverordnung – Praxiserfahrungen und Evaluation Aus der Sicht von Datenschutzbeauftragten“, in: Datenschutz und Datensicherheit 05/2020, S. 297.
[12] Vgl. *Die Landesbeauftragte für den Datenschutz Niedersachsen*: „Querschnittsprüfung Abschlussbericht November 2019“, URL: https://lfd.niedersachsen.de/download/14930, S. 13, Abruf 16.09.2020.

ist eine Hilfstätigkeit, bei der die Hauptaufgabe bei dem Verantwortlichen verbleibt. Gemäß Art. 4 Nr. 8 DS-GVO bleibt der Verantwortliche i.S.d. Gesetzes auch im Rahmen einer Auftragsverarbeitung grundsätzlich für die Verarbeitung verantwortlich. Die Auftragsverarbeitung soll dadurch gerade kein datenschutzrechtliches „Rundum-sorglos-Paket" darstellen.[13] Diese Form der Datenverarbeitung erleichtert die Arbeitsteilung jedoch ungemein und ist nicht nur in der Privatwirtschaft, sondern auch im öffentlichen Sektor sehr weit verbreitet.[14] Hierdurch kann externes Spezialwissen einfacher einbezogen und effektiver gewirtschaftet werden. Der Verantwortliche hat hierbei die Pflicht, vor der Auswahl eines Auftragsverarbeiters zu überprüfen, ob dieser geeignete TOMs getroffen hat. Weiterhin muss er sich während des Verlaufs des Auftragsverarbeitungsverhältnisses versichern, dass diese geeigneten TOMs aufrechterhalten werden.[15] Es handelt sich dabei um eine fortwährende Überprüfungspflicht.[16] Die Überprüfung jedes Auftragsverarbeiters vor Vertragsabschluss sowie die regelmäßigen Kontrollen und Sicherstellung geeigneter TOMs bei sämtlichen Auftragsverarbeitern während der Laufzeit des Auftragsverarbeitungsverhältnisses sind für den Verantwortlichen meist sehr schwer umzusetzen. Solche Kontrollen sind mit einem sehr hohen Personalaufwand verbunden. Hinzu kommen teilweise mangelhafte Fachkenntnisse und fehlendes Bewusstsein in den Unternehmen. Laut der Querschnittsprüfung der Landesbeauftragten für den Datenschutz Niedersachsen schnitten die Unternehmen zum Thema Verständnis von geeigneten TOMs überdurchschnittlich schlecht ab und nur die Hälfte erwähnte das Bewusstsein, für die Schutzmaßnahmen auch bei den Auftragsverarbeitern verantwortlich zu sein.[17] Dies zeigt die vorhandenen Defizite und die Bedeutung der Entwicklung von adäquaten Lösungen in diesem Bereich auf.

Diese beiden Kernthemen, das Recht auf Löschung gemäß Art. 17 DS-GVO in Verbindung mit dem Erfordernis zur Erstellung eines Löschkonzeptes und die Auftragsverarbeitung bezüglich der Kontrolle der TOMs gemäß Art. 28 DS-GVO sind Hauptgegenstand dieser Studie. Die zum Teil sehr abstrakten datenschutzrechtlichen Vorgaben stellen die Unternehmen bei der Umsetzung der Anforderungen in verschiedenen Bereichen oftmals vor Probleme. Für Einige ist dies auch trotz vorhandenem Bewusstsein für die jeweiligen Themen aufgrund fehlender Konzepte, Kenntnisse und Kapazitäten unternehmensintern nicht möglich. Das Ziel besteht darin, die durch datenschutzrechtliche Anforderungen hervorgerufenen betrieblichen Herausforderungen im Hinblick auf Datenlöschung und Auftragsverarbeitung zu durchleuchten und Handlungsempfehlungen abzuleiten. Dadurch sollen praxisorientierte und verständliche Hinweise und Konzepte zur Umsetzung dieser Aspekte formuliert werden. Zu Beginn werden mit Blick auf den Untersuchungsgegenstand die grundlegenden datenschutzrechtlichen Anforderungen dargestellt. Im anschließenden Abschnitt werden die betrieblichen Herausforderungen in der Praxis erörtert und verdeutlicht. Durch Interviews mit erfahrenen Datenschutzexperten aus verschiedenen Branchen sollen die praxisrelevanten Schwachstellen identifiziert werden. Folgend wird auf die Problemstellungen Recht auf Löschung und

[13] Vgl. *Der Bayerische Landesbeauftragte für den Datenschutz*: „Aktuelle Kurz-Information 6 - Keine gesonderte Entgeltpflicht für Kontrollen bei der Auftragsverarbeitung", URL: https://www.datenschutz-bayern.de/datenschutzreform2018/aki06.pdf, S. 1, Abruf 13.01.2021.
[14] Vgl. *Der Bayerische Landesbeauftragte für den Datenschutz*: „Auftragsverarbeitung – Orientierungshilfe", URL: https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf, S. 1, Abruf 13.01.2021.
[15] Vgl. *Plath, Kai-Uwe,* in: Plath, Kai-Uwe (Hrsg.): DSGVO/BDSG, 3. Aufl., Otto Schmidt, Köln 2018, Art. 28 Rn. 8.
[16] Vgl. *Martini, Mario,* in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 2. Aufl., C.H. Beck, München 2018, DS-GVO Art. 28 Rn. 21.
[17] Vgl*. Die Landesbeauftragte für den Datenschutz Niedersachsen*: „Querschnittsprüfung Abschlussbericht November 2019", URL: https://lfd.niedersachsen.de/download/14930, S. 13 f., Abruf 16.09.2020.

Kontrolle der TOMs im Rahmen der Auftragsverarbeitung eingegangen und mögliche Lösungen und Vorgehensweisen entwickelt und analysiert. Schließlich wird jeweils eine Handlungsempfehlung für die betriebliche Praxis zu diesen beiden Themenbereichen abgeleitet. Im Fazit erfolgt eine Reflexion der erarbeiteten Erkenntnisse.

2 UNTERSUCHUNGSGEGENSTAND

Zur Untersuchung der Problemstellungen hinsichtlich der Umsetzung des Rechts auf Löschung und der Kontrolle der TOMs bei einem Auftragsverarbeiter in der betrieblichen Praxis werden zunächst die hierfür notwendigen datenschutzrechtlichen Anforderungen dargestellt. Des Weiteren ist die Kenntnis der praktischen Bedürfnisse zur Entwicklung einer optimalen Lösung unverzichtbar.

2.1 DATENSCHUTZRECHTLICHE ANFORDERUNGEN

Die DS-GVO und einige darin enthaltenen Grundlagen und allgemeinen Bestimmungen zu den datenschutzrechtlichen Anforderungen bieten das Grundgerüst, um die Zusammenhänge und Hintergründe der Fragestellungen zu analysieren und Lösungen erarbeiten zu können.

DS-GVO:

Die DS-GVO ersetzt die EG-Datenschutzrichtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Das Ziel der EG-Datenschutzrichtlinie war, das Datenschutzniveau innerhalb der EU anzugleichen. Dies konnte jedoch aufgrund des, bei einer Richtlinie notwendigen Umsetzungsrechtsakts in jedem einzelnen EU-Mitgliedstaat nicht erreicht werden.[18] In Erwägungsgrund 9 zur DS-GVO werden die, aus der unterschiedlichen Handhabung resultierenden Rechtsunsicherheiten als Hemmnis für die unionsweite Ausübung von Wirtschaftstätigkeiten beschrieben, die den Wettbewerb verzerren und die Behörden an der Erfüllung der ihnen nach dem Unionsrecht obliegenden Pflichten hindern. Danach besitzen die Ziele der alten EG-Datenschutzrichtlinie trotz der unterschiedlichen Umsetzung weiterhin Gültigkeit. Durch die direkte Wirkung von Verordnungen und damit der DS-GVO sollen nun die Harmonisierung des Datenschutzniveaus innerhalb der EU und die Rechtssicherheit in Bezug auf grenzüberschreitende Verarbeitungsvorgänge gewährleistet werden. An einigen Stellen enthält die DS-GVO Öffnungsklauseln, durch die die Mitgliedstaaten einen gewissen Spielraum haben, mit dem sie datenschutzrechtliche Vorgaben ausgestalten und spezifischere Regelungen erlassen können.[19] Zunächst muss also immer von den Vorschriften der DS-GVO ausgegangen werden, jedoch muss zudem ermittelt werden, ob in den Gesetzen der einzelnen Mitgliedstaaten spezielle nationale Regeln zur Anwendung kommen.[20] Dieser Grundsatz ist bei den, im Rahmen dieser Arbeit behandelten Themen ein wichtiger Aspekt. Darüber hinaus können in bestimmten Fällen weitere Vorschriften anderer Rechtsgebiete und Gesetze Auswirkungen auf die datenschutzrechtlichen Prozesse haben, worauf im späteren Verlauf näher eingegangen wird.

[18] Vgl. *Voigt, Paul; von dem Bussche, Axel*: EU-Datenschutz-Grundverordnung (DSGVO): Praktikerhandbuch, Springer, Wiesbaden 2018, S. 1 ff.
[19] Vgl. *Ehman, Eugen; Selmayr, Martin,* in: Ehmann, Eugen; Selmayr, Martin (Hrsg.): DS-GVO, 2. Aufl., C.H. Beck, München 2018, Einf. Rn. 82 ff.
[20] Vgl. *Forgó, Nikolaus; Helfrich, Marcus; Schneider, Jochen,* in: Forgó, Nikolaus; Helfrich, Marcus; Schneider, Jochen (Hrsg.): Betrieblicher Datenschutz. Rechtshandbuch, 3. Aufl., C.H. Beck, München 2019, Teil I. Kapitel 5. Grundsätze der datenschutzrechtlichen Prüfung Rn. 5 ff.

Seit Inkrafttreten der DS-GVO gibt es immer wieder Unsicherheiten hinsichtlich der Erwägungsgründe, der Gesetzesformulierungen und der Übersetzung in die Sprachen der EU-Mitgliedstaaten. Dennoch hat sich die Verordnung in vielen Bereichen als wertvoll und weitsichtig erwiesen und hat einen stark harmonisierenden Effekt.[21] Das Grundrecht zum Schutz personenbezogener Daten findet sich in Art. 8 Abs. 1 Charta der Grundrechte der Europäischen Union (GRCh) wieder. Dieses Recht wird durch Abs. 2 in gewisser Weise eingeschränkt. Danach dürfen personenbezogene Daten nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Damit wird das Verbot mit Erlaubnisvorbehalt zum Ausdruck gebracht. Abs. 3 schreibt die Überwachung des Datenschutzes durch eine unabhängige Stelle vor. Neben Art. 8 GRCh (Schutz personenbezogener Daten) wendet der EuGH in seinen Entscheidungen meist Art. 7 GRCh (Schutz des Privat- und Familienlebens) an. Die Erwägungsgründe lehnen sich ebenfalls an Art. 8 GRCh an, jedoch ziehen Erwägungsgrund 1 und 12 zur DS-GVO Art. 16 AEUV heran, der den Schutz personenbezogener Daten regelt und als formelle Ermächtigungsgrundlage der Verordnung dient.[22] Art. 1 DS-GVO nennt den Gegenstand und die Ziele der Verordnung und geht dabei auf die Grundrechte und Grundfreiheiten von natürlichen Personen ein. Sie enthält demnach Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten. Sie schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. Zusätzlich darf der freie Verkehr personenbezogener Daten in der Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden. Dadurch soll sichergestellt werden, dass der Datenaustausch unionsweit in gleicher Weise wie innerhalb der Mitgliedstaaten frei bleibt.[23] Der breite Anwendungsbereich hat sowohl direkte als auch indirekte Auswirkungen auf Staaten außerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR). Bei der Datenübermittlung aus der EU in Staaten außerhalb der EU/des EWR betrifft es die diese sogenannten Drittländer direkt, da die personenbezogenen Daten nicht ohne bestimmte Sicherheiten transferiert werden dürfen. Art. 44 DS-GVO stellt die allgemeinen Grundsätze der Datenübermittlung auf. Danach ist eine Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in den folgenden Artikeln aufgeführten Bedingungen einhalten und auch die sonstigen Bestimmungen der Verordnung beachtet werden. Nach Art. 45 DS-GVO dürfen personenbezogene Daten beispielsweise an ein Drittland außerhalb der EU/des EWR übermittelt werden, wenn die EU-Kommission dem jeweiligen Land ein angemessenes Datenschutzniveau bescheinigt. Dabei wird somit zwischen sicheren und unsicheren Drittländern unterschieden. Bisher wurde nur wenigen Ländern ein angemessenes Datenschutzniveau zugesprochen, diese sind: Andorra, Argentinien, Kanada (nur kommerzielle Organisationen), Färöer, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Schweiz, Uruguay oder zuletzt Japan.[24] Da die personenbezogenen Daten auch in unsichere Drittländer wie z. B. Indien übermittelt werden, müssen z.B. geeignete Garantien aus Art. 46 DS-GVO vorgesehen wer-

[21] Vgl. *Weichert, Thilo*: „Die DSGVO, ein – ganz guter – Anfang“, in: Datenschutz und Datensicherheit, 05/2020, S. 293.
[22] Vgl. *Ernst, Stefan,* in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 2. Aufl., C.H. Beck, München 2018, DS-GVO Art. 1 Rn. 4 ff.
[23] Vgl. *ebd.*, Art. 1 Rn. 14
[24] Vgl. *European Commission*: “Adequacy decisions - How the EU determines if a non-EU country has an adequate level of data protection”, URL: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, Abruf 18.09.2020.

den. Eine indirekte Wirkung hat die DS-GVO durch die Vorbildwirkung für Staaten, die mit EU-Mitgliedstaaten Geschäfte abwickeln. Das brasilianische Datenschutzrecht orientiert sich an der DS-GVO und selbst in Afrika fungiert die Verordnung als Beispiel.[25] Ein wichtiges Hilfsmittel für die Durchsetzung und Einhaltung der DS-GVO und ein Grund für die gestiegene Aufmerksamkeit und das erhöhte Bewusstsein ist die Möglichkeit abschreckende Bußgelder zu verhängen. Art. 83 DS-GVO schreibt konkret Sanktionen für bestimmte verwaltungsrechtliche Verstöße gegen die Verordnung vor. In Art. 84 DS-GVO werden von den Mitgliedstaaten Sanktionen für Verstöße gefordert, die von diesem Artikel nicht erfasst werden. Dies betrifft mehrheitlich strafrechtliche Sanktionen, die nur von den Mitgliedstaaten beschlossen werden können.[26] Ein wichtiges Instrument zur Überprüfung möglicher Defizite, der Einleitung geeigneter Maßnahmen und zur Modernisierung der Verordnung sind die Berichte der Kommission gemäß Art. 97 Abs. 1 DS-GVO.[27] Diese Norm schreibt der Kommission vor, bis zum 25. Mai 2020 und danach alle vier Jahre dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung der Verordnung vorzulegen. Art. 97 Abs. 2 DS-GVO enthält eine nicht abschließende Liste der zu überprüfenden Punkte. Gemäß Art. 97 Abs. 5 DS-GVO müssen bei diesen Vorgängen aufgrund der Wichtigkeit dieser Thematik in der heutigen Zeit insbesondere die Entwicklungen in der Informationstechnologie und die Fortschritte in der Informationsgesellschaft berücksichtigt werden. Dieser Aspekt ist insbesondere für die Umsetzung des Rechts auf Löschung von großer Bedeutung. Diese Regelungen zeigen die Erkenntnis, dass die Digitalisierung Wirtschaft, Staat und Gesellschaft sehr rasant und langfristig verändert und der Schutz der Werte dabei erhalten und damit immer wieder angepasst werden soll.[28]

Personenbezogene Daten:

Die Anwendbarkeit der DS-GVO bestimmt sich nach dem sachlichen Anwendungsbereich und damit einhergehend nach dem Vorliegen einer Verarbeitung personenbezogener Daten.[29] Art. 2 Abs. 1 DS-GVO eröffnet den Anwendungsbereich für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten und die nicht automatisierte Verarbeitung, sofern die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Gemäß Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen. Als identifizierbar gilt eine natürliche Person demnach, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standorten, 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, identifiziert werden kann. Der Wortlaut „alle Informationen“ soll eine weite Auslegung des Begriffs zum Ausdruck bringen.[30] Als identifiziert i.S.d. Gesetzes gilt eine Person also, wenn ein Iden-

[25] Vgl. *Weichert, Thilo*: „Die DSGVO, ein – ganz guter – Anfang“, in: Datenschutz und Datensicherheit, 05/2020, S. 294.
[26] Vgl. *Boehm, Franziska,* in: Simitis, Spiros; Hornung, Gerrit; Spiecker, Indra (Hrsg.): Datenschutzrecht. DSGVO mit BDSG, Nomos, Baden-Baden 2019, Art. 83 Rn. 1ff.
[27] Vgl. *Roßnagel, Alexander*: „Evaluation der Datenschutz-Grundverordnung Verfahren – Stellungnahmen – Vorschläge“, in: Datenschutz und Datensicherheit, 05/2020, S. 287.
[28] Vgl. *Roßnagel, Alexander*: „Evaluation nutzen!“, in: Datenschutz und Datensicherheit, 05/2020, S. 281.
[29] Vgl. *Wächter, Michael*: Datenschutz im Unternehmen, 5. Auflage, C.H. Beck, München 2017, S. 134.
[30] Vgl. *Art. 29 – Datenschutzgruppe*: „WP 136. Begriff der personenbezogenen Daten“, URL: https://datenschutz.hessen.de/infothek/europäischer-datenschutzausschuss-artikel-29-datenschutzgruppe, S. 7, Abruf: 24.09.2020.

tifikationsmerkmal wie beispielsweise der Name oder das Geburtsdatum vorliegt und somit zur Identifikation keine weiteren Informationen benötigt werden.[31] Eine Abgrenzung von personenbezogenen zu nicht personenbezogenen Daten ist in der Praxis oftmals sehr schwierig. Insbesondere herrschen Unklarheiten, auf wen bei der Beurteilung der Identifizierbarkeit abzustellen ist. Dabei werden zwei verschiedene Ansätze diskutiert. Der relative Ansatz geht ausschließlich bei der Identifizierbarkeit für den Verantwortlichen von einem Personenbezug aus, während der absolute Ansatz die Identifizierbarkeit durch einen Dritten bereits als ausreichend ansieht.[32] Erwägungsgrund 26 S. 3 zur DS-GVO lässt auf einen absoluten Ansatz hindeuten. Demnach ist unerheblich, ob der Verantwortliche selbst in der Lage ist, die natürliche Person zu identifizieren und es genügt, wenn dies für eine andere (dritte) Person nach allgemeinem Ermessen wahrscheinlich möglich ist. In der Literatur wird hingegen oft der relative Ansatz bevorzugt.[33] Laut Brink/Eckhardt wird dem Verantwortlichen der Kenntnisstand eines Dritten zugerechnet, wenn eine Zusammenführung der Kenntnisse rechtlich möglich, von beiden Seiten gewollt und wahrscheinlich zu erwarten ist.[34] Der EuGH schlägt in einer ersten leichten Anmerkung zu diesem Thema in gewisser Weise einen Mittelweg ein, in dem er auf das Wissen und die Mittel Dritter abstellt.[35] Eine optimale Lösung wird sich wohl aus Bestandteilen beider Theorien ergeben. Hinsichtlich der Auslegung herrscht also nach wie vor Unklarheit. Gemäß dem Erwägungsgrund sind ebenso die zur Verfügung stehenden Mittel zu bewerten, die zur Identifizierung nach allgemeinem Ermessen wahrscheinlich genutzt werden. Bei der Prüfung sollten gemäß Erwägungsgrund 26 S. 4 zur DS-GVO unter Einbeziehung der zum Zeitpunkt der Verarbeitung verfügbaren Technologie und der technologischen Entwicklung zusätzlich alle objektiven Faktoren wie die Kosten und der Zeitaufwand berücksichtigt werden. Die Beurteilung der Identifizierbarkeit muss stets aktuell gehalten werden, da die Faktoren je nach Person und Situation unterschiedlich bewertet werden müssen.[36] Im Kontext der Ausgestaltung und der Anforderungen an die Löschung personenbezogener Daten und mit Blick auf TOMs wie die Pseudonymisierung ist diese Beurteilung und Abgrenzung von enormer Wichtigkeit.

Technische und organisatorische Maßnahmen:

Die Bezeichnung „technische und organisatorische Maßnahmen“ ist an mehreren Stellen der DS-GVO wiederzufinden.[37] Während Art. 32 DS-GVO dabei die Gesamtheit aller TOMs umfasst, wird Art. 24 DS-GVO als „Generalnorm der Verantwortungszuweisung“[38] verstanden.[39]

---

[31] Vgl. *Klar, Manuel; Kühling, Jürgen,* in: Buchner, Benedikt; Kühling, Jürgen (Hrsg.): Datenschutz-Grundverordnung/BDSG, 2. Aufl., C.H. Beck, München 2018, Art. 4 Nr. 1 Rn. 18.
[32] Vgl. *Schwartmann, Rolf; Mühlenbeck, Robin L.,* in: Schwartmann, Rolf; Jaspers, Andreas; Thüsing, Gregor; Kugelmann, Dieter (Hrsg.): DS-GVO/BDSG. Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, C.F. Müller, Heidelberg 2018, Art. 4 Nr. 1 Rn. 23.
[33] Vgl. *Klar, Manuel; Kühling, Jürgen,* in: Buchner, Benedikt; Kühling, Jürgen (Hrsg.): Datenschutz-Grundverordnung/BDSG, 2. Aufl., C.H. Beck München 2018, Art. 4 Rn. 25.
[34] Vgl. *Brink, Stefan; Eckhardt, Jens*: „Wann ist ein Datum ein personenbezogenes Datum? Anwendungsbereich des Datenschutzrechts“, in: Zeitschrift für Datenschutz, 05/2015, S. 211.
[35] Vgl. *EuGH,* Urteil vom 19.10.2016, C-582/14, juris, Rn. 31 ff.
[36] Vgl. *Laue, Philip,* in: Laue, Philip, Kremer, Sascha (Hrsg.): Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl., Nomos, Baden-Baden 2019, S. 40.
[37] Vgl. *Keber, Tobias O.; Keppeler, Lutz Martin,* in: Schwartmann, Rolf; Jaspers, Andreas; Thüsing, Gregor; Kugelmann, Dieter (Hrsg.): DS-GVO/BDSG. Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, C.F. Müller, Heidelberg 2018, Art. 25 Rn. 31.
[38] Vgl. *Martini, Mario,* in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 2. Aufl., C.H. Beck, München 2018, DS-GVO Art. 24 Rn. 1.
[39] Vgl. *Husemann, Charlotte,* in: Roßnagel, Alexander: “Das neue Datenschutzrecht. Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze“, Nomos, Baden-Baden 2018, S. 168.

Die technischen Maßnahmen beziehen sich auf den Datenverarbeitungsvorgang, die organisatorischen Maßnahmen regeln dagegen die äußeren Rahmenbedingungen.[40] Durch diese Maßnahmen erfolgt die praktische, aufgrund der unbestimmten Rechtsbegriffe oft sehr komplexe Umsetzung des Datenschutzes.[41] Der Gesetzgeber schreibt im Gesetzeswortlaut und in dem dazugehörigen Erwägungsgrund lediglich geeignete TOMs mit Pseudonymisierung als Beispiel vor, um Datenschutzgrundsätze wie z. B. die Datenminimierung umzusetzen. Eine Öffnungsklausel zur Konkretisierung in den nationalen Gesetzen wie dem Bundesdatenschutzgesetz (BDSG) wurde nicht aufgenommen.[42] Um die hier behandelte Kontrolle der TOMs bei den Auftragsverarbeitern korrekt durchführen zu können, müssen bestimmte Anhaltspunkte zur Bewertung herangezogen werden können. Wie die TOMs faktisch auszusehen haben, muss anhand der folgenden Kriterien aus den Art. 24 Abs. 1, 32 Abs. 1 DS-GVO abgeleitet werden:

- Stand der Technik:

  Den aktuellen Stand der Technik zu bestimmen ist, nicht immer einfach. Von dem Begriff selbst kann keine konkrete Aussage abgeleitet werden. Hartung beschreibt damit „Technologien, die auf gesicherten Erkenntnissen beruhen und in der Praxis jeweils bereits in ausreichendem Maß zur Verfügung stehen, um angemessen umgesetzt zu werden“.[43] Aufgrund der ständigen Weiterentwicklung ändert sich der Stand der Technik sehr häufig und muss kontinuierlich neu bewertet werden.

- Implementierungskosten:

  Bei der Auswahl von geeigneten TOMs spielt auch der Kostenfaktor eine tragende Rolle. Hier muss eine Abwägung der Verhältnismäßigkeit vorgenommen werden, der Verantwortliche muss keine Maßnahmen ergreifen, die nur einen geringen Mehrwert leisten, hingegen aber unverhältnismäßig hohe Kosten mit sich bringen. Die Nichteinhaltung der Datenschutzgrundsätze gemäß Art. 5 DS-GVO kann damit jedoch nicht gerechtfertigt werden, sondern lediglich die Auswahl einer Maßnahme.[44]

- Art, Umfang, Umstände und Zweck der Verarbeitung, Eintrittswahrscheinlichkeit und Schwere der Risiken:

  Gemäß Erwägungsgrund 76 zur DS-GVO sind die Art, der Umfang und der Zweck keine kumulativen Merkmale, sondern dienen der Bewertung der Eintrittswahrscheinlichkeit und der Schwere der Risiken. Anhand einer objektiven Bewertung soll das Risiko in Kategorien von „Risiko“ bis „hohes Risiko“ klassifiziert werden. Erwägungsgrund 75 zur DS-GVO liefert hierfür eine nicht abschließende Liste von Risiken für die Rechte und Freiheiten natürlicher Personen. Durch die Berührung mit Art. 24 DS-GVO und Art. 32 DS-GVO können auch die dort angeführten Maßnahmen wie die

[40] Vgl. *Martini, Mario,* in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 2. Aufl., C.H. Beck, München 2018, DS-GVO Art. 25 Rn. 28.
[41] Vgl. *Schmieder, Fabian,* in: Forgó, Nikolaus; Helfrich, Marcus; Schneider, Jochen (Hrsg.): Betrieblicher Datenschutz. Rechtshandbuch, 3. Aufl., C.H. Beck, München 2019, S. 1322 f.
[42] Vgl. *Baumgartner, Ulrich; Gausling, Tina*: „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“, in: Zeitschrift für Datenschutz, 07/2017, S. 310.
[43] *Hartung, Jürgen,* in: Buchner, Benedikt; Kühling, Jürgen (Hrsg.): Datenschutz-Grundverordnung/BDSG, 2. Aufl., C.H. Beck München 2018, Art. 25 Rn. 21.
[44] Vgl. *Martini, Mario,* in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 2. Aufl., C.H. Beck, München 2018, DS-GVO Art. 25 Rn. 41 f.

Verschlüsselung oder Zugangskontrollen herangezogen werden.[45] Die Artikel-29-Datenschutzgruppe hat in ihrem Working Paper 168 eine Orientierungshilfe für manche Bereiche wie z. B. die öffentliche Videoüberwachung bereitgestellt.[46] Nach Art. 25 Abs. 1 DS-GVO müssen, wie in Form der Datenminimierung exemplarisch genannt, die Datenschutzgrundsätze aus Art. 5 Abs. 1 DS-GVO durch diese Maßnahmen wirksam umgesetzt werden.[47]

Datenschutzgrundsätze und Erlaubnistatbestände:

Art. 5 Abs. 1 DS-GVO legt die Datenschutzgrundsätze fest, die in Verbindung mit Art. 6 DS-GVO die Voraussetzungen für den datenschutzkonformen Umgang mit personenbezogenen Daten festlegen. Die Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 DS-GVO sind:

- Rechtmäßigkeit der Verarbeitung,
- Verarbeitung nach Treu und Glauben,
- Transparenz der Verarbeitung,
- Zweckbindung der Verarbeitung,
- Datenminimierung,
- Richtigkeit,
- Speicherbegrenzung,
- Integrität und
- Vertraulichkeit.

Einige dieser Grundsätze werden in verschiedenen Artikeln der DS-GVO immer wieder genannt wie die Rechtmäßigkeit, die Verarbeitung nach Treu und Glauben und die Transparenz aus Art. 5 Abs. 1 lit. a) DS-GVO. Auf andere jedoch wird im weiteren Verlauf nicht mehr eingegangen. Art. 5 Abs. 1 lit. d) DS-GVO und damit der Grundsatz der Richtigkeit wird beispielsweise im weiteren Verlauf nicht mehr erwähnt.[48] Diese Norm schreibt allerdings vor, personenbezogene Daten müssen, sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein und es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden. Somit ist diese Vorschrift gleichwohl in vielen Bereichen enorm wichtig, insbesondere auch bei dem nachfolgend behandelten Recht auf Löschung. Art. 5 DS-GVO regelt allerdings nicht das „Ob“, sondern das „Wie“ der gesetzeskonformen Durchführung einer Datenverarbeitung. Das „Ob“ und somit die Zulässigkeit

[45] Vgl. *Hartung, Jürgen,* in: Buchner, Benedikt; Kühling, Jürgen (Hrsg.): Datenschutz-Grundverordnung/BDSG, 2. Aufl., C.H. Beck München 2018, Art. 25 Rn. 16.
[46] Vgl. *Art. 29 – Datenschutzgruppe*: „WP 168. Die Zukunft des Datenschutzes – gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten“, URL: https://www.bfdi.bund.de/SharedDocs/Publikationen/EU/Art29Gruppe/WP168_de.html?cms_submit=Senden&cms_templateQueryString=wp+168, S. 16, Abruf: 05.10.2020.
[47] Vgl. *Wennemann, Thomas*: „TOM und die Datenschutz-Grundverordnung“, in: Datenschutz und Datensicherheit, 01/2018. S. 177.
[48] Vgl. *Forgó, Nikolaus; Helfrich, Marcus; Schneider, Jochen,* in: Forgó, Nikolaus; Helfrich, Marcus; Schneider, Jochen (Hrsg.): Betrieblicher Datenschutz. Rechtshandbuch, 3. Aufl., C.H. Beck, München 2019, Kapitel 5. Grundsätze der datenschutzrechtlichen Prüfung Rn. 40 ff.

der Verarbeitung personenbezogener Daten wird in Art. 6 Abs. 1, Art. 9 Abs. 2 und Art. 10 DS-GVO reglementiert.[49]

Die DS-GVO enthält kein eigenes Verbotsprinzip, wie häufig zu lesen ist.[50] Das Verbot, nicht ohne Rechtfertigung in Grundrechte eingreifen zu dürfen, gilt für das Datenschutzrecht wie für alle anderen Grundrechte auch.[51] Dadurch muss also einer der Erlaubnistatbestände gemäß Art. 6 Abs. 1 DS-GVO vorliegen, im Fall von besonderen Kategorien personenbezogener Daten eben Art. 9 DS-GVO bzw. bei Daten über strafrechtliche Verurteilungen und Straftaten Art. 10 DS-GVO. Nach den überwiegend anzuwendenden Erlaubnistatbeständen gemäß Art. 6 Abs. 1 ist eine Verarbeitung personenbezogener Daten in folgenden Fällen rechtmäßig: durch eine Einwilligung der betroffenen Person, zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen, zur Erfüllung einer rechtlichen Verpflichtung, zum Schutz lebenswichtiger Interessen, zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt oder wenn die Verarbeitung zur Wahrung berechtigter Interessen erforderlich ist. Die dadurch erlaubte Verarbeitung muss dann unter Beachtung der Datenschutzgrundsätze umgesetzt werden. Ein Verstoß gegen die Datenschutzgrundsätze bedeutet nicht grundsätzlich die Unzulässigkeit der Verarbeitung, jedoch wird sie dadurch rechtswidrig.

2.2 Betriebliche Herausforderungen in der Praxis

Die DS-GVO und die darin enthaltenen datenschutzrechtlichen Anforderungen stellen die Unternehmen im Zuge der Umsetzung des Rechts auf Löschung und der Auftragsverarbeitung, wie bereits erwähnt, häufig vor große Herausforderungen. Um die Ursachen zu erforschen und optimale Empfehlungen aussprechen zu können, sind ein Einblick in die Praxis und die Erfahrungen von Experten unabdingbar. Vor diesem Hintergrund wurden Interviews mit Experten aus verschiedenen Brachen geführt, mit dem Ziel, das tatsächliche Verbesserungspotential in der Praxis zu identifizieren und zu verdeutlichen. Anhand der Ergebnisse sollen Lösungen für die betriebliche Praxis erarbeitet werden.

Dabei wurde das explorative Experteninterview als qualitative Methode zur Schärfung des Problembewusstseins angewendet. Die Experten sollten damit in dem Gespräch den Handlungszusammenhang im betrieblichen datenschutzrechtlichen Umfeld darstellen. Sie sind dabei selbst ein Teil des zu untersuchenden Handlungsfeldes. Dadurch konnten Informationen aus dem Umfeld des Untersuchungsbereichs und technisches und Prozesswissen der Experten gesammelt werden. Das explorative Interview wurde möglichst offen geführt, um ein breites Spektrum an Informationen zu erhalten.[52] Durch die Befragung dreier Experten aus der Banken- und Versicherungs-, Beratungs- und Automobilbranche konnten branchenübergreifende Interpretationen und Sichtweisen bzw. Abläufe erörtert werden. Zunächst wurde ein Leitfaden mit konkreten Fragen entwickelt und in die beiden Themen Recht auf Lö-

[49] Vgl. *Roßnagel, Alexander*: „Datenschutzgrundsätze – unverbindliches Programm oder verbindliches Recht? Bedeutung der Grundsätze für die datenschutzrechtliche Praxis“, in: Zeitschrift für Datenschutz, 08/2018, S. 343.
[50] Vgl. *Schulz, Sebastian,* in: Gola, Peter (Hrsg.): Datenschutz-Grundverordnung, 2. Aufl., C.H. Beck, München 2018, Art. 6 Rn. 2.
[51] Vgl. *Roßnagel, Alexander,* in: Roßnagel, Alexander: “Das neue Datenschutzrecht. Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze“, Nomos, Baden-Baden 2018, § 3 Rn. 50.
[52] Vgl. *Bogner, Alexander; Littig, Beate; Menz, Wolfgang*: „Interviews mit Experten - Eine praxisorientierte Einführung“, in: Bohnsack, Ralf; Flick, Uwe; Lüders, Christian; Reichertz, Jo (Hrsg.): Qualitative Sozialforschung, Springer Fachmedien, Wiesbaden 2014, S. 22 ff.

schung und Auftragsverarbeitung, jeweils mit den Unterpunkten zu Herausforderungen und möglichen Vorgehensweisen, gegliedert. Der Leitfaden diente in der Erhebungssituation als Orientierung, um dem Gespräch eine Struktur zu verleihen. Im Vorfeld des Interviews wurde der Leitfaden an die Interviewpartner versandt, um ihnen einen Überblick über die entsprechenden Themen zu bekommen. Die darin enthaltenen Fragestellungen stellten dabei keineswegs ein Redeskript dar, sondern dienten lediglich der Gedächtnisstütze und der inhaltlichen und methodischen Vorbereitung.[53] Für die Auswertung wurde die qualitative Inhaltsanalyse herangezogen, um die Zustände und Prozesse in der Praxis zu identifizieren. Die Interviewtexte wurden derart umgebaut und in Kategorien eingeordnet, dass die Informationen verwendbar dargestellt werden können. Im ersten Schritt erfolgte die Materialauswahl, dabei wurde der Text nach stichhaltigen Informationen selektiert. Im zweiten Schritt wurde ein Kategoriensystem entwickelt, welches verschiedene Kategorien und die Beziehungen zueinander enthält. Bei der Extraktion ging es im dritten Schritt um die thematische Ordnung der relevanten Informationen, um eine einheitliche Informationsbasis zu schaffen. Die Daten wurden hier den Kategorien zugeordnet. Im letzten Schritt wurden die Daten aufbereitet und zusammenhängende Informationen aus den unterschiedlichen Interviews zusammengetragen.[54] Somit konnten die tatsächlichen Herausforderungen in den alltäglichen Abläufen identifiziert werden.

Bei den Aufsichtsbehörden steht die fristgerechte und gesetzeskonforme Löschung aufgrund der enormen Anzahl an Verarbeitungen personenbezogener Daten in den Unternehmen im Fokus. [55] Der Landesbeauftragte für Datenschutz und Informationsfreiheit in Baden-Württemberg Stefan Brink betont in der Praxis ebenfalls immer wieder die Wichtigkeit und Schwierigkeit dieses Themas. Im Rahmen der Experteninterviews haben sich Herausforderungen hervorgehoben, die sich bei der Umsetzung in der betrieblichen Praxis ergeben. Die Aufmerksamkeit und das Bewusstsein der betroffenen Personen zu diesem Thema sind laut der übereinstimmenden Darstellungen der Experten gestiegen. Dies hat insbesondere unmittelbar nach Inkrafttreten der DS-GVO zu einem Anstieg im Bereich der Anfragen zu Löschbegehren geführt. Um diesem Recht der betroffenen Personen adäquat nachkommen zu können, werden klare Abläufe benötigt. Die Löschbegehren erreichen eine Organisation oftmals über viele verschiedene Kanäle. Die Schwierigkeiten bestehen bereits im Erkennen des Löschbegehrens, der Weiterleitung an die zuständige Stelle und dem Identifizieren der personenbezogenen Daten der jeweils betroffenen Person. Vergleichsweise kommen solche Anfragen jedoch selten bzw. überwiegend bei Berufsbewerbern und im Rahmen des Newsletter-Versand zum Tragen. Der größere Aufwand ergibt sich aufgrund der Häufigkeit und der Datenmengen aus der systematischen Löschung im Falle einer Zweckerfüllung oder der weiteren gesetzlich festgelegten Gründe unabhängig von Anträgen auf Löschung durch betroffene Personen. Ein wichtiger Schritt besteht hier darin, alle personenbezogenen Daten und deren Speicherort zu identifizieren. Wie auch bei Löschbegehren stellt dies eine große Herausforderung dar. Dieser Schritt erfordert von beiden Prozessen eine ähnliche Vorgehensweise. In den Unternehmen besteht eine heterogene Systemlandschaft mit einer Vielzahl an Systemen, was das Identifizieren erschwert. Eine vollständige Übersicht zu erstellen, stellt die Praxis vor eine nahezu unlösbare Aufgabe, insbesondere auch, weil Mitarbeiter Dokumente mit personenbezogenem Inhalt häufig zusätzlich lokal auf ihren Rechnern abge-

[53] Vgl. *Bogner, Alexander; Littig, Beate; Menz, Wolfgang*: „Interviews mit Experten - Eine praxisorientierte Einführung“, in: Bohnsack, Ralf; Flick, Uwe; Lüders, Christian; Reichertz, Jo (Hrsg.): Qualitative Sozialforschung, Springer Fachmedien, Wiesbaden 2014, S. 27 f.
[54] Vgl. *ebd.*, S. 73.
[55] Vgl. *Ingelheim, Alexander*: „Das erste Jahr DSGVO - Eine Bestandsaufnahme“, in: *Controlling & Management Review* 63, 04/2019, S. 69.

speichert haben. Teilweise ist das Bewusstsein für solche Verarbeitungsvorgänge bei den Mitarbeitern nicht ausreichend, wodurch die Identifizierung zusätzlich verkompliziert wird. Den lokalisierten Daten müssen im weiteren Verlauf Aufbewahrungsfristen zugeordnet werden. Die DS-GVO schreibt keine konkreten Fristen vor, wann eine Zweckerfüllung eintritt und welche Aufbewahrungsfristen darüber hinaus einschlägig sind. Die Vorschriften hierzu müssen aus den jeweiligen nationalen Gesetzgebungen abgeleitet werden. In einem internationalen Konzern können dadurch sehr komplexe Situationen entstehen und durch verbundene Unternehmen in den verschiedensten Ländern der Welt viele unterschiedliche Vorschriften zur Anwendung kommen. Zusätzlich ist das Festlegen von starren Fristen in der Praxis kaum möglich. Zu geringe Fristen sind durch die Zwecke der Verarbeitung nicht umsetzbar und zu lange Fristen sind datenschutzrechtlich nicht vertretbar.[56] Erschwerend kommt die mögliche Nutzung von personenbezogenen Daten zu mehreren Zwecken hinzu, wodurch die Daten im Falle einer Zweckerfüllung gegebenenfalls für einen anderen Zweck weiterhin gespeichert werden müssen.[57] Im letzten Schritt stellt die Definition des Begriffs der Löschung, d.h. die Umsetzung einer tatsächlichen Löschung i.S.d. Gesetzes die Unternehmen vor gewisse Probleme. Auf der einen Seite bereitet das rein physische Löschen z.B. durch Schreddern nur wenige Schwierigkeiten, auf der anderen Seite wirft das technische Löschen in den Systemen einige Fragen auf. Bei vielen Softwareanbietern ist eine endgültige Löschung nicht möglich und Daten können entweder lediglich überschrieben werden oder zumindest der Anbieter kann diese zu jeder Zeit wiederherstellen. Bisher wurde bei der Auswahl der Software in den Unternehmen höchst selten auf die Möglichkeit einer praktikablen Löschung mit der Definition von unterschiedlichen Fristen geachtet.[58] In der Praxis werden die bestmöglichen Anstrengungen unternommen, um die gesetzlichen Anforderungen zu erfüllen, jedoch herrscht diesbezüglich eine allseitige Ungewissheit. Bei einem Großteil der Unternehmen dauern die Projekte zur Umsetzung der Anforderungen bezüglich des Rechts auf Löschung auch mehr als zwei Jahre nach wirksam werden der Verordnung noch immer an.

Auch das Themenfeld der Auftragsverarbeitung und die damit verbundene gesetzliche Verpflichtung einer regelmäßigen Kontrolle der technischen und organisatorischen Maßnahmen beim Auftragsverarbeiter führt in der Praxis zu Herausforderungen. Das Verhältnis Auftraggeber und Auftragsverarbeiter ist vertraglich zu regeln. Dabei ergeben sich in der Praxis Schwierigkeiten bei der Abgrenzung zwischen einer Auftragsverarbeitung und einer gemeinsamen Verantwortlichkeit oder sogar von eigenen Verantwortlichkeiten der Beteiligten jeweils i.S.d. Gesetzes. Unter anderem aus diesem Grund werden Auftragsverarbeitungsverträge auch teilweise pro forma geschlossen. Eine weitere Ursache ist die Unsicherheit durch fehlende Kenntnisse der rechtlichen Vorgaben. In diesen Fällen erfolgt überwiegend auch keine Überprüfung der TOMs, wodurch der Zweck in Frage gestellt werden kann und gegen die gesetzlichen Vorgaben verstoßen wird. Die Verantwortlichen haben Probleme eine Überprüfung bei allen Auftragsverarbeitern durchzusetzen. Dieser Vorgang ist mit hohem Aufwand verbunden und benötigt eine große personelle Kapazität. Große Konzerne nehmen eine Vielzahl an Auftragsverarbeitern in Anspruch, von denen jeder einzelne kontrolliert werden muss. Die Überprüfung muss darüber hinaus nicht nur vor der Beauftragung bzw. dem Vertragsschluss erfolgen, sondern weiterhin turnusmäßig während des gesamten Auftragsverarbeitungsverhältnisses. Um eine vollständige und regelmäßige Kontrolle durchführen zu

[56] Vgl. *Deutsches Institut für Normung e.V. (Hrsg.)*: DIN 66398, Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Beuth Verlag, Berlin 2016, S. 27.
[57] Vgl. *Berning, Wilhelm; Keppeler, Lutz Martin*: „Technische und rechtliche Probleme bei der Umsetzung der DS-GVO Löschpflichten“, in: Zeitschrift für Datenschutz, 07/2017, S. 317.
[58] Vgl. *ebd.*, S. 314.

können, wird in vielen Fällen eine eigene Einheit in dem Unternehmen benötigt. Dies ist für eine überwiegende Anzahl der Akteure unter anderem aus wirtschaftlichen Gründen nicht umsetzbar und ein risikobasierter Ansatz wird angewendet. Durch den Einsatz von Fragebögen zu den TOMs als Self-Assessment besteht das Risiko, dass die entsprechenden Antworten die Wirklichkeit nicht korrekt abbilden. Im Falle nicht hinreichender Garantien für geeignete TOMs darf die Zusammenarbeit nicht eingegangen bzw. muss diese beendet werden. Bei speziellen Dienstleistern mit exklusiven Leistungen, die zwingend benötigt werden, kann dies weitreichende Folgen haben und die Unternehmen vor große Probleme stellen. Sollten die Auftragsverarbeiter anerkannte Zertifizierungen i.S.d. Gesetztes vorlegen können, werden die TOMs von vielen Verantwortlichen trotzdem zusätzlich überprüft, wodurch der Aufwand dennoch nicht reduziert wird. Um Lösungen für diese praktischen Herausforderungen erarbeiten zu können, werden im Folgenden zunächst die speziellen konzeptionellen Grundlagen der angesprochenen Themen dargestellt.

3 KONZEPTIONELLE GRUNDLAGEN

Um die notwendigen Schritte und Anforderungen ableiten zu können, müssen die detaillierten konzeptionellen Grundlagen bezogen auf die hier behandelten Themen erörtert werden. Nur anhand dieses Hintergrunds kann eine gesetzeskonforme praktische Umsetzung erfolgen.

3.1 RECHT AUF LÖSCHUNG

3.1.1 Verpflichtung zur Erstellung eines Löschkonzepts

Aufgrund des enormen Umfangs und der großen Anzahl an Verarbeitungen personenbezogener Daten schreiben die Datenschutzbehörden der gesetzeskonformen Umsetzung des Rechts auf Löschung eine hohe Bedeutung zu und stellen diese in den Fokus.[59] Für unrechtmäßige Datenverarbeitungsvorgänge oder solche, die unrichtige oder unvollständige Daten betreffen, sieht die DS-GVO Betroffenenrechte zum Schutz der Rechte und Freiheiten der Betroffenen Personen vor.[60] Hierzu zählt auch die wohl am meisten diskutierte Regelung der Verordnung, das Recht auf Löschung. In der DS-GVO wird dieses auch als „Recht auf Vergessenwerden“ bezeichnet. In der Google Spain Entscheidung des EuGH vom 13.05.2014 wurde ein Fall gegen den Suchmaschinenanbieter diesbezüglich bejaht und damit der Grundstein für ein effektiveres Recht auf Vergessenwerden gelegt. Nach geltendem Recht bestehe demnach ein begrenzter Anspruch des Betroffenen auf Löschung der personenbezogenen Daten. Voraussetzung sei in diesem Fall ein Antrag des Betroffenen sowie eine Abwägung der schutzwürdigen Interessen des Betroffenen mit dem Informationsinteresse der Öffentlichkeit an der Verbreitung der Information zugunsten des Betroffenen.[61] Im seit dem 25.05.2018 und aktuell geltenden Recht wird das Recht auf Löschung in Art. 17 DS-GVO geregelt. Dieses Betroffenenrecht wird auch häufig als Internet-Grundrecht bezeichnet und geht über die Verpflichtungen der Google Spain Entscheidung hinaus. Die Löschverpflichtungen sind nicht derart neu, wie sie die mediale Präsenz auf den ersten Blick erscheinen lässt. Auch die EG-Datenschutzrichtlinie und das Bundesdatenschutzgesetz alte Fas-

[59] Vgl. *Ingelheim, Alexander*: „Das erste Jahr DSGVO - Eine Bestandsaufnahme“, in: Controlling & Management Review 63, 04/2019, S. 69.
[60] Vgl. *Voigt, Paul; von dem Bussche, Axel*: EU-Datenschutz-Grundverordnung (DSGVO): Praktikerhandbuch, Springer, Wiesbaden 2018, S. 206.
[61] Vgl. *EuGH,* Urteil vom 13.5.2014, C-131/12, GRUR 2014, S. 895.

sung (BDSG a.F.) enthalten bereits solche Regelungen.[62] Art. 17 DS-GVO regelt somit die Verpflichtung zur Löschung personenbezogener Daten. Dabei hat gemäß Abs. 1 eine Löschung zu erfolgen, wenn:

- die personenbezogenen Daten für die Zwecke der Verarbeitung nicht mehr notwendig sind. Hier wurden die Daten zunächst rechtmäßig erhoben und verarbeitet, jedoch sind sie für den Verarbeitungszweck nicht mehr notwendig oder dieser wird nicht mehr weiterverfolgt.[63]
- eine Einwilligungserklärung widerrufen wird und keine andere Rechtsgrundlage für die Verarbeitung vorhanden ist. Eine betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen.[64]
- die betroffene Person legt gemäß Art. 21 Abs. 1 DS-GVO Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Art. 21 Abs. 2 DS-GVO Widerspruch ein. Gemäß Art. 21 Abs. 1 DS-GVO kann eine betroffene Person einer auf öffentlichem oder berechtigtem Interesse beruhenden Verarbeitung auf Grundlage ihrer Umstände und der konkreten Situation widersprechen, wenn sie die Umstände der veränderten Interessenlage darlegen kann. Gemäß Art. 21 Abs. 2 DS-GVO kann die betroffene Person einer Verarbeitung für Zwecke der Direktwerbung widersprechen.[65]
- die Verarbeitung unrechtmäßig erfolgte, z.B. bei einer fehlenden Rechtsgrundlage oder dem Verstoß gegen sonstige Vorschriften der DS-GVO.[66]
- die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich ist, dem der Verantwortliche unterliegt.
- die Daten in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Abs. 1 DS-GVO (Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft) erhoben wurden. Gemäß Erwägungsgrund 65 zur DS-GVO sollen damit personenbezogene Daten von Kindern geschützt werden, da die betroffene Person ihre Einwilligung noch im Kindesalter gegeben hat und die mit der Verarbeitung verbundenen Gefahren nicht in vollem Umfang absehen konnte und die personenbezogenen Daten – insbesondere die im Internet gespeicherten – später löschen möchte.

Art. 17 Abs. 2 DS-GVO regelt die Löschung veröffentlichter personenbezogener Daten. Der Verantwortliche hat geeignete Maßnahmen zur Information anderer Verantwortlicher über die Löschung zu treffen. Hierbei kommt es nach Art. 17 Abs. 2 DS-GVO nicht auf den Erfolg an[67], sondern viel mehr auf die, unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessenen Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren. Die Angemessenheit hängt dabei auch von der Art und Weise der Verarbeitung der personenbezogenen Daten und der Beeinträchtigung der Betroffenenrechte ab. Je grö-

[62] Vgl. *Paal, Boris P.*, in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 2. Aufl., C.H. Beck, München 2018, BDSG Art. 17 Rn. 2.
[63] Vgl. *Worms, Christoph,* in: Brink, Stefan; Wolff, Heinrich Amadeus (Hrsg.): BeckOK Datenschutzrecht, 33. Edition, C.H. Beck, München 2020, Art. 17 Rn. 25.
[64] Vgl. *Voigt, Paul; von dem Bussche, Axel*: EU-Datenschutz-Grundverordnung (DSGVO): Praktikerhandbuch, Springer, Wiesbaden 2018, S. 209 f.
[65] Vgl. *ebd.*, S. 210.
[66] Vgl. *ebd.*
[67] Vgl. *Paal, Boris P.,* in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 2. Aufl., C.H. Beck, München 2018, BDSG Art. 17 Rn. 32.

ßer die Beeinträchtigung, desto größer der Aufwand der von dem Verantwortlichen erwartet werden kann. Da es sich überwiegend um Online-Veröffentlichungen handelt kann beispielsweise in jedem Fall verlangt werden, die wichtigsten Suchmaschinenanbieter über das Löschverlangen zu informieren. Die Informierten selbst können dadurch gemäß Art. 17 Abs. 1 DS-GVO zur Löschung verpflichtet sein, Abs. 2 begründet jedoch keinen Löschungsanspruch in sich selbst. Das Ziel der Norm besteht vielmehr darin, den informierten Verantwortlichen bösgläubig zu machen.[68] Daneben muss der Verantwortliche gemäß Art. 19 DS-GVO bei einer begrenzten Zahl an Empfängern, allen, denen Daten offengelegt wurden, die Löschung mitteilen, sofern dies nicht unmöglich oder mit unverhältnismäßigem Aufwand verbunden ist. Der Umfang und die Bedeutung für die betroffene Person muss dabei mit dem Aufwand für den Verantwortlichen abgewogen werden.[69]

Art. 17 Abs. 3 DS-GVO enthält Ausnahmetatbestände zu den Abs. 1 und 2. Danach gelten diese nicht, wenn die Verarbeitung erforderlich ist,

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information. Hierdurch soll die große verfassungsrechtliche Streitfrage durch das Aufeinandertreffen der verschiedenen Positionen in der Praxis in Einklang gebracht werden.[70] Dies kann auch als eine Folge des Google Spain-Urteils und der damit verbundenen Diskussion um die Informationsinteressen der Öffentlichkeit verstanden werden.[71] Nach der nicht umstrittenen Ansicht der Kommission kann sich ein Suchmaschinenbetreiber allerdings nicht auf dieses Recht berufen.[72]
- zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Dieser Ausnahmetatbestand enthält eine Öffnungsklausel für die Mitgliedstaaten, beispielsweise bei steuer- oder handelsrechtlichen Aufbewahrungspflichten.[73]
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3.
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Die dargestellten Löschpflichten aus Art. 17 DS-GVO können auf Basis des Art. 23 Abs. 1 DS-GVO unter bestimmten Bedingungen beschränkt werden. Der deutsche Gesetzgeber macht davon in § 35 BDSG Gebrauch. Ist eine Löschung im Falle nicht automatisierter Da-

[68] Vgl. *Dix, Alexander,* in: Simitis, Spiros; Hornung, Gerrit; Spiecker, Indra (Hrsg.): Datenschutzrecht. DSGVO mit BDSG, Nomos, Baden-Baden 2019, Art. 17 Rn. 28.
[69] Vgl. *Mantz, Reto; Marosi, Johannes*, in: Specht, Louisa; Mantz, Reto (Hrsg.): Handbuch Europäisches und deutsches Datenschutzrecht, 1. Aufl., C.H. Beck, München 2019, S. 69 Rn. 128 f.
[70] Vgl. *Paal, Boris P.,* in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 2. Aufl., C.H. Beck, München 2018, BDSG Art. 17 Rn. 41.
[71] Vgl. *Roßnagel, Alexander; Nebel, Maxi; Richter, Philipp*: „Was bleibt vom Europäischen Datenschutzrecht?
Überlegungen zum Ratsentwurf der DS-GVO“, in: Zeitschrift für Datenschutz, 10/2015, S. 455.
[72] Vgl. *Paal, Boris P.,* in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 2. Aufl., C.H. Beck, München 2018, BDSG Art. 17 Rn. 42.
[73] Vgl. *Braun, Martin; Kamann, Hans-Georg,* in: Ehmann, Eugen; Selmayr, Martin (Hrsg.): DS-GVO, 2. Aufl., C.H. Beck, München 2018, Art. 17 Rn. 53.

tenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung personenbezogener Daten gemäß Artikel 17 Abs. 1 DS-GVO ergänzend zu den in Artikel 17 Abs. 3 DS-GVO genannten Ausnahmen nach dieser Vorschrift nicht. Die Löschung wird in einem solchen Fall mit der Einschränkung der Verarbeitung nach Art. 18 DS-GVO ersetzt und die Daten werden gesperrt. Da jedoch keines der in Art. 23 Abs. 1 DS-GVO als Voraussetzung genannten Schutzziele auf diese Abweichung von der Verordnung zutrifft, ist diese Regelung möglicherweise unionsrechtlich angreifbar. Zusätzlich wirkt die DS-GVO gemäß Art. 2 Abs. 1 Var. 1 unmittelbar für die „nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“, daher ist § 35 BDSG so auszulegen, dass er nur in Fällen, in denen keine Speicherung in Dateisystemen erfolgte oder erfolgen sollte, anzuwenden ist.[74]

Das Recht auf Löschung sieht mit Ausnahme von nicht automatisierter Verarbeitung keine Verhältnismäßigkeitsprüfung für Verantwortliche vor, wie sie im BDSG a.F. noch verankert war. Dies führt bei vielen Verantwortlichen zu großem Unmut im Zusammenhang mit der Erstellung eines Löschkonzepts. Hier wird häufig mit betriebswirtschaftlichen Aspekten argumentiert, wobei die große Bedeutung und Wichtigkeit dieses Rechts jedoch nicht in Frage gestellt wird.[75] Sofern also einer der genannten Löschungsgründe vorliegt, müssen die jeweiligen personenbezogenen Daten gemäß Art. 17 Abs. 1 DS-GVO ohne die Möglichkeit einer Verhältnismäßigkeitsprüfung unverzüglich gelöscht werden. Die in Art. 12 Abs. 4 DSGVO geregelte allgemeine Frist bei der Ausübung der Rechte der betroffenen Personen von maximal einem Monat wird durch diese Vorschrift und in diesem Fall verdrängt. Der Verantwortliche ist dem Wortlaut nach auch von sich aus und unabhängig von einem Antrag einer betroffenen Person zur Löschung der Daten verpflichtet. Das Löschungsrecht der betroffenen Personen korreliert dabei mit der Löschungspflicht des Verantwortlichen.[76] Für die verschiedenen Kategorien personenbezogener Daten erfordert diese Verpflichtung in der Praxis das Festlegen unterschiedlicher Löschfristen.[77] Dadurch entsteht ein Spannungsfeld zwischen den Regelungen in der DS-GVO zu Datensparsamkeit und Löschung und den legitimen bzw. gesetzlich vorgeschriebenen Aufbewahrungspflichten. Der Verantwortliche muss alle personenbezogenen Daten auf das Vorliegen von Löschungsgründen und das mögliche Zutreffen eines Ausnahmetatbestandes in den speziellen Einzelfällen überprüfen. Ein solcher Vorgang kann mehrere Tage in Anspruch nehmen.[78]

Gerade im digitalen Zeitalter stellt sich häufig die Frage, welche Anforderungen an eine Löschung in der Praxis konkret gestellt werden. Art. 4 Nr. 2 DS-GVO erwähnt den Begriff als Form einer Verarbeitung, definiert ihn jedoch nicht näher und auch in den Erwägungsgründen werden keine weiteren Anhaltspunkte gegeben. In der Literatur haben sich jedoch einige Ansätze gebildet. Eine Löschung i.S.d. Gesetztes erfordert je nach Art der Aufbewah-

[74] Vgl. Martini, Mario, in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 1. Aufl., C.H. Beck, München 2017, DS-GVO Art. 30 Rn. 18a.
[75] Vgl. *Schulz, Sebastian*: „Die Evaluation der DSGVO - Anregungen aus dem Maschinenraum“, in: Datenschutz und Datensicheheit, 05/2020, S. 305.
[76] Vgl. Kremer, Sascha, in: Laue, Philip, Kremer, Sascha (Hrsg.): Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl., Nomos, Baden-Baden 2019, S. 177.
[77] Vgl. *Worms, Christoph,* in: Brink, Stefan; Wolff, Heinrich Amadeus (Hrsg.): BeckOK Datenschutzrecht, 33. Edition, C.H. Beck, München 2020, Art. 17 Rn. 54.
[78] Vgl. *Voigt, Paul; von dem Bussche, Axel*: EU-Datenschutz-Grundverordnung (DSGVO): Praktikerhandbuch, Springer, Wiesbaden 2018, S. 216.

rung der Daten eine physische Vernichtung bzw. Unbrauchbarmachung oder im Fall von elektronischen Daten eine technische Löschung.[79] Nach herrschender Meinung wird darauf abgestellt, dass personenbezogene Daten nicht mehr verarbeitet und nicht ohne übermäßigen Aufwand wiederhergestellt werden können bzw. die Daten nicht mehr ohne übermäßigen Aufwand wahrgenommen werden können.[80] Die personenbezogenen Daten können auch vollständig anonymisiert bzw. bei pseudonymen Daten der zugehörige Schlüssel entfernt werden.[81] Bei einer Anonymisierung bleibt der Gehalt der Daten erhalten, jedoch kann keine Zuordnung zu einer bestimmten oder bestimmbaren Person mehr erfolgen.[82] Die personenbezogenen Daten müssen derart anonymisiert werden, dass die Anonymisierung nicht mehr umkehrbar ist.[83] Gemäß Erwägungsgrund 26 zur DS-GVO werden die datenschutzrechtlichen Grundsätze nicht auf anonyme Daten angewendet. Zur Feststellung, ob die Anonymisierung umkehrbar ist und ob eine Person identifizierbar ist, müssen gemäß dem Erwägungsgrund die dafür zur Verfügung stehenden Mittel bewertet werden, die nach allgemeinem Ermessen wahrscheinlich genutzt werden. Bei der Feststellung, ob die Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten dem Erwägungsgrund zufolge alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand herangezogen werden. Dabei sind die zum Zeitpunkt der Verarbeitung verfügbare Technologie und die technologischen Entwicklungen zu berücksichtigen. Die mögliche Wiederherstellung mit Hilfe von Spezialprogrammen beeinflusst die Löschung ebenfalls nach herrschender Meinung nicht.[84] Durch die ständigen Veränderungen und technischen Fortschritte, müssen die Anforderungen an eine Löschung fortlaufend angepasst werden.[85] Eine besonders große Herausforderung stellt die Blockchain-Technologie dar, welche bei Kryptowährungen, Smart Contracts, dem Grundbuch, dem Handelsregister oder als Grundlage für das Internet der Dinge zur Anwendung kommen kann und die Digitalisierung auf die nächste Stufe heben soll. Vereinfacht und nur kurz dargestellt ist eine Blockchain eine dezentral geführte Datenbank, bei der Transaktionsdaten in einer Kette verknüpfter Blöcke gespeichert werden. Die Datenkette ist auf allen teilnehmenden Rechnern gespeichert, welche sich gegenseitig kontrollieren. Durch den Validierungsprozess und die Verknüpfung der Blöcke durch einzigartige sogenannte Hash-Werte sind die Daten nicht nachträglich veränderbar und stellen eine enorm sichere Technologie dar. Fraglich ist in diesem Zusammenhang, ob eine Blockchain personenbezogene Daten verarbeitet, wer der Verantwortliche ist und wie die Betroffenenrechte durchgesetzt werden können. Eine Blockchain enthält zwar lediglich pseudonymisierte Daten wie die Hash-Werte, jedoch finden die datenschutzrechtlichen Vorschriften auch auf pseudonymisierte Daten An-

[79] Vgl. *Paal, Boris P.,* in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 2. Aufl., C.H. Beck, München 2018, BDSG Art. 17 Rn. 30.
[80] Vgl. *Härting, Niko*: Datenschutz-Grundverordnung: Das neue Datenschutzrecht in der betrieblichen Praxis, 1. Aufl., Verlag Dr. Otto Schmidt 2016, Rn. 701; *Nolte, Norbert; Werkmeister, Christoph,* in: Gola, Peter (Hrsg.): Datenschutz-Grundverordnung, 2. Aufl., C.H. Beck, München 2018, Art. 17 Rn. 8.
[81] Vgl. Peuker, Enrico, in: Sydow, Gernot: Europäische Datenschutzgrundverordnung, 2. Aufl., Nomos, Baden-Baden 2018, Art. 17 Rn. 32.
[82] Vgl. *Ernst, Stefan,* in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 2. Aufl., C.H. Beck, München 2018, DS-GVO Art. 4 Rn. 49.
[83] Vgl. *Art. 29 – Datenschutzgruppe*: „WP 216 Stellungnahme 5/2014 zu Anonymisierungstechniken“, URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf, S. 7 ff., Abruf: 10.12.2020.
[84] Vgl. *Hennemann, Moritz*: „Das Recht auf Löschung gemäß Art. 17 Datenschutz-Grundverordnung“, in: PinG, 05/2016, S. 176; *Braun, Martin; Kamann, Hans-Georg,* in: Ehmann, Eugen; Selmayr, Martin (Hrsg.): DS-GVO, 2. Aufl., C.H. Beck, München 2018, Art. 17 Rn. 55.
[85] Vgl. *Bundesamt für die Sicherheit in der Informationstechnik*: „Daten richtig löschen“, URL: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/richtigloeschen_node.html, Abruf: 14.10.2020.

wendung. Denn mit Hilfe von Zusatzinformationen können in dem System nähere Daten ermittelt werden.[86] Aufgrund der dezentralen Speicherung kommen mehrere Verantwortliche in Betracht. Beispielsweise kommen zum einen alle Mitglieder des Netzwerks und zum anderen derjenige der die Blockchain programmiert oder initiiert in Frage. Gemäß Art. 4 Nr. 7 DS-DVO ist Verantwortlicher, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Somit sind alle Nodes, also alle Teilnehmer des Netzwerks Verantwortliche, da sie den Zweck der Teilnahme verfolgen und Daten verarbeiten.[87] Die Unveränderbarkeit und die lückenlose Speicherung stehen in Konflikt mit dem Recht auf Löschung und der Durchsetzung des Betroffenenrechts.[88] Diesbezüglich wird viel über Möglichkeiten und neue Ansätze diskutiert, die jedoch noch nicht derart ausgereift sind und für eine erfolgreiche Durchsetzung der Rechte der Betroffenen weiterentwickelt werden müssen.[89]

Alternativ zum Recht auf Löschung steht den betroffenen Personen unter den Voraussetzungen des Art. 18 Abs. 1 DS-GVO das Recht auf Einschränkung der Verarbeitung zur Wahl. Dies kann in einigen Fällen praktikabler für die Betroffen sein, worauf hier aber nicht weiter eingegangen werden soll.

Im Zuge der Rechtsdurchsetzung haben betroffene Personen gemäß Art. 77 DS-GVO das Recht auf Beschwerde bei einer Aufsichtsbehörde oder das Recht auf einen gerichtlichen Rechtsbehelf, woraufhin der Vorgang gerichtlich überprüft wird. Im Falle eines Verstoßes gegen die Vorschriften des Art. 17 Abs. 1 und Abs. 2 DS-GVO kommt nach Art. 83 Abs. 5 lit. b) DS-GVO ein Bußgeldrahmen von bis zu 20.000.000 EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres eines Unternehmens zur Anwendung. Dabei ist der jeweils höhere Betrag maßgebend. Zusätzlich kann die zuständige Aufsichtsbehörde gemäß Art. 58 Abs. 2 lit. c) DS-GVO und Art. 58 Abs. 2 lit. g) DS-GVO den Verantwortlichen anweisen, den Anträgen der betroffenen Personen zu entsprechen und die Löschung durchzuführen.

In der Praxis führen die Löschvorgaben häufig zu großen Herausforderungen. Viele Verantwortliche haben keine klaren Regeln definiert, um eine Löschung gesetzeskonform umzusetzen. Zusätzlich sind viele IT-Systeme bisher nicht darauf ausgelegt und es bestehen Schwierigkeiten bei der technischen Umsetzung. Die fehlenden Kenntnisse der Mitarbeiter oder die laienhafte Annahme die Daten könnten in Zukunft nochmals gebraucht werden, was aber unbestimmte Zwecke beschreibt und damit nicht zulässig ist, tragen ebenfalls dazu bei. Erschwerend kommen auch die oftmals sehr komplexen Zusammenhänge der Daten durch die Verarbeitung in mehreren Prozessen und zu mehreren Zwecken hinzu.[90] Die Bedeutung der gesetzlichen Verpflichtung zur Erstellung eines Löschkonzeptes wurde am 30. Oktober 2019 durch den Bußgeldbescheid in Höhe von 14,5 Millionen Euro der Berliner Beauftragten für Datenschutz und Informationsfreiheit gegen die Deutsche Wohnen SE hervorgehoben. Bei der Speicherung personenbezogener Daten der Mieterinnen und Mieter wurde laut der Pressemitteilung der Berliner Beauftragten für Datenschutz und Informationsfreiheit ein System

[86] Vgl. *Bechtolt, Hans; Vogt, Niklas*: „Datenschutz in der Blockchain – Eine Frage der Technik“, in: Zeitschrift für Datenschutz 02/2018, S. 66.
[87] So iE auch die Einordnung von Suchmaschinenbetreibern, *EuGH*, EuZW 2014, S. 541 f.
[88] Vgl. *Martini, Mario; Weinzierl, Quirin*: „Die Blockchain-Technologie und das Recht auf Vergessenwerden: zum Dilemma zwischen Nicht-Vergessen-Können und Vergessen-Müssen“, in: NvWZ 17/2017, S. 1251 ff.
[89] Vgl. *Bechtolf, Hans; Vogt, Niklas*: „Datenschutz in der Blockchain – Eine Frage der Technik“, in: Zeitschrift für Datenschutz 02/2018, S.69 f.
[90] Vgl. *Hammer, Volker*: DIN 66398 - Die Leitlinie Löschkonzept als Norm, in: Datenschutz und Datensicherheit, 08/2016, S. 528.

verwendet, mit dem es nicht möglich war, nicht mehr benötigte Daten zu löschen. Die personenbezogenen Daten wurden gespeichert, ohne zu überprüfen, ob dies zulässig und erforderlich ist.[91] Laut Erwägungsgrund 39 S. 10 zur DS-GVO soll der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen, um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden. In der betrieblichen Praxis kann ein solcher Prozess nur durch klar definierte Vorgehensweisen sichergestellt werden. Um gesetzeskonform zu agieren, können die Abläufe nur in Form eines speziellen Löschkonzepts umgesetzt werden.[92] Die Pflicht zur Erstellung eines Löschkonzepts ergibt sich zusätzlich unter anderem aus den Datenschutzgrundsätzen Erforderlichkeit, Speicherbegrenzung und Datenminimierung gemäß Art. 5 Abs. 1 DS-GVO.[93] Die Vorgänge und beispielsweise die identifizierten Löschfristen bezüglich dieses Prozesses müssen ebenfalls dokumentiert werden, um einen Nachweis darüber erbringen zu können. Grundsätzlich ergibt sich aus den Art. 5, 24 DS-GVO eine Rechenschaftspflicht auch für das Recht auf Löschung. Gemäß Art. 5 Abs. 2 DS-GVO muss die Einhaltung der Anforderungen der Verordnung nachgewiesen werden können. Art. 24 DS-GVO legt die Notwendigkeit geeigneter TOMs fest, um nachzuweisen, dass die Vorgaben der DS-GVO eingehalten werden. Dabei reicht ein Nachweis einzig über das Verzeichnis der Verarbeitungstätigkeiten oder des Grundsatzes der Datenminimierung nicht aus.[94] Die Dokumentationspflicht und damit die Dokumentationsanforderungen wurden durch die Vorschriften bezüglich der Rechenschaftspflicht deutlich verschärft und können nicht hoch genug eingeschätzt werden.[95] Insbesondere sollen dadurch für die Aufsichtsbehörden bessere Möglichkeiten der Überprüfung geschaffen werden. Des Weiteren schreibt Art. 30 Abs. 1 lit. f) DS-GVO vor, die Löschfristen der verschiedenen Datenkategorien „wenn möglich“, in das Verfahrensverzeichnis aufzunehmen. Davon kann ausgegangen werden, wenn dies „ohne unzumutbaren Aufwand und in einer nicht völlig sinnfreien Weise umsetzbar ist“.[96] Auch im Rahmen des Art. 25 DS-GVO zum Datenschutz durch Technikgestaltung und durch Datenschutzfreundliche Voreinstellungen wird ausdrücklich die Berücksichtigung von Speicherfristen bei der Umsetzung der Voreinstellungen erwähnt. Somit müssen die Speicherfristen klar formuliert und von den beteiligten Personen eingesehen werden können. Im Hinblick auf die Informationspflichten aus Art. 13 Abs. 2 lit. a) DS-GVO und Art. 14 Abs. 2 lit. a) DS-GVO müssen den betroffenen Personen bei der Erhebung personenbezogener Daten die Dauer der Speicherung oder zumindest die Kriterien für die Festlegung dieser Dauer mitgeteilt werden, was aufgrund der benötigten Informationen gleichermaßen eines solchen Konzepts bedarf. Ebenso müssen diese Informationen die Rechtsgrundlage und den Zweck der Verarbeitung beinhalten. Damit soll den Betroffenen die Ausübung ihrer Rechte erleichtert werden.[97] Um diesen Dokumentations- und Nachweispflichten gerecht werden zu können, ist die systematische Dokumentation anhand eines

[91] Vgl. *Berliner Beauftragte für Datenschutz und Informationsfreiheit*: Pressemitteilung 711.412.1 v. 05.11.2019.
[92] Vgl. *Berning, Wilhelm; Keppeler, Lutz Martin*: „Technische und rechtliche Probleme bei der Umsetzung der DS-GVO Löschpflichten“, in: Zeitschrift für Datenschutz, 07/2017, S. 315.
[93] Vgl. *Auer-Reinsdorff, Astrid; Conrad Isabell*: Handbuch IT- und Datenschutzrecht, 3. Auflage, C.H. Beck, München 2019, Rn. 615.
[94] Vgl. *Lachenmann, Matthias,* in: Lachenmann, Matthias; Koreng, Ansgar (Hrsg.): Formularhandbuch Datenschutzrecht, 2.Aufl., C.H. Beck, München 2018, A.I Rechenschaftspflicht (Art. 5, 24 DS-GVO) Rn. 1ff.
[95] Vgl. *Jung, Alexander*: „Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO“, Zeitschrift für Datenschutz, 05/2018, S. 208.
[96] Vgl. *Martini, Mario,* in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 1. Aufl., C.H. Beck, München 2017, DS-GVO Art. 30 Rn. 18c.
[97] Vgl. *Schneider, Jochen*: Datenschutz nach der EU-Datenschutz-Grundverordnung, 2. Aufl., C.H. Beck, München 2019, S. 193.

Löschkonzepts unausweichlich.[98] Die Inhalte eines Löschkonzepts sind also gleichzeitig, sowohl für einen funktionierenden Prozess als auch zur Erfüllung der Dokumentations- und Nachweispflichten, erforderlich. Ein Löschkonzept stellt einen wichtigen Teilbereich eines Datenschutz-Managementsystems eines Unternehmens dar. Der Begriff Datenschutz-Managementsystem wird in der Verordnung und den dazugehörigen Erwägungsgründen zwar nicht erwähnt, jedoch ergibt sich beispielsweise aus den Vorschriften des Art. 24 DS-GVO indirekt eine Verpflichtung zur Implementierung eines solchen.[99] Somit wird der Begriff in diesem Zusammenhang auch nicht definiert. Das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein beschreibt das System und dessen Anforderungen in seinen Hinweisen zur Dokumentation einer ordnungsgemäßen Verarbeitung personenbezogener Daten folgendermaßen:

„Es ist ein organisationsweites Datenschutz-Managementsystem zu betreiben (Artikel 24 Absatz 1 und Artikel 32 Absatz 1 Buchstabe d DSGVO, § 12 Absatz 3 Nr. 7 LDSG), das sowohl der kontinuierlichen Gewährleistung der Wirksamkeit der Datenschutzmaßnahmen und deren Prüfbarkeit dient als auch auf Änderungen solcher Umstände reagiert, die sich auf Verarbeitungen personenbezogener Daten auswirken können. Das Datenschutz-Managementsystem ist zu dokumentieren. Dazu gehören mindestens Aussagen

- über die Bereitstellung von Ressourcen,
- zur Einbindung der oder des behördlichen Datenschutzbeauftragten in die Organisation des Verantwortlichen, in die Planung von Verarbeitungstätigkeiten und in Datenschutz-Folgenabschätzungen (Artikel 35 DSGVO),
- zur Vorgehensweise in Bezug auf Prüfungen laufender Verarbeitungstätigkeiten, insbesondere der Wirksamkeit der technisch-organisatorischen Datenschutzmaßnahmen,
- zur Vorgehensweise in Bezug auf die Ergebnisse solcher Prüfungen (Festlegung und Umsetzung von Korrekturmaßnahmen) sowie
- zur Vorgehensweise in Bezug auf die Maßnahmen zum Erfüllen von Rechten betroffener Personen einschließlich der Beschäftigten (Artikel 12 bis 22 DSGVO bzw. §§ 31-35 LDSG).“[100]

Unter letztgenanntem Punkt „Vorgehensweise in Bezug auf die Maßnahmen zum Erfüllen von Rechten betroffener Personen“ ist auch das Recht auf Löschung zu zählen. Wie bereits erläutert, muss die Vorgehensweise diesbezüglich in Form eines Löschkonzepts dokumentiert werden, welches somit auch nach dieser Ansicht in ein Datenschutz-Managementsystem aufgenommen werden muss. Ein einheitlicher Standard wie etwa im Kontext eines Compliance-Managementsystems wurde bisher allerdings noch nicht eingeführt. Die DIN 29100 wird zwar als Norm hierzu gesehen, ihr fehlt aber ein „klarer Handlungsauftrag“, um solch ein System anhand dessen aufbauen zu können. Häufig wird auch die Verwendung der ISO 27001 unter der Ergänzung von Datenschutzbausteinen vorgeschlagen. Diese Norm zielt grundsätzlich auf ein Informationssicherheits-Managementsystem ab und ist zu unspezifisch für die Anforderungen der DS-GVO. Für die Überprüfung der TOMs kann die Norm je-

[98] Vgl. *Jung, Alexander*: „Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO“, Zeitschrift für Datenschutz, 05/2018, S. 208.
[99] Vgl. *Berning, Wilhelm; Keppeler, Lutz Martin*: „Technische und rechtliche Probleme bei der Umsetzung der DS-GVO Löschpflichten“, in: Zeitschrift für Datenschutz, 07/2017, S. 317.
[100] Vgl. *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*: „Hinweise zur Dokumentation einer ordnungsgemäßen Verarbeitung personenbezogener Daten“, URL: https://www.datenschutzzentrum.de/uploads/dokumentation/Hinweise_zur_Dokumentation.pdf, S. 6 Abruf: 08.01.2021.

doch bereits herangezogen werden.[101] Hinsichtlich der Nachweis- und Dokumentationspflichten sollte innerhalb eines Unternehmens also ein Datenschutz-Managementsystem aufgebaut werden oder zumindest bereits Strukturen in Richtung eines solchen Systems erkennbar sein.[102] In einem Unternehmen sind die Daten meist in großem Umfang in allen Bereichen vorhanden, wodurch es sehr schwierig wird, ohne ein geeignetes Konzept den Überblick zu behalten.[103] Aus diesen Normen kann abgeleitet werden, dass ein Datenschutz-Managementsystem und damit einhergehend ein Löschkonzept nunmehr als „Pflicht und nicht mehr als Kür“[104] angesehen werden muss. Um die genannten Herausforderungen bezüglich der Löschung vor diesem Hintergrund meistern zu können und den gesetzlichen Anforderungen gerecht zu werden, müssen innerhalb der Organisation klare Prozesse und Abläufe definiert werden. Ebenso müssen die genannten Dokumentations- und Nachweispflichten erfüllt werden. Daraus ergibt sich auch die Notwendigkeit der Dokumentation in Form eines Löschkonzepts zur Erfüllung des in Art. 17 DS-GVO geregelten Rechts auf Löschung und der weiteren genannten einschlägigen Vorschriften hierzu.

Weder die DS-GVO noch das BDSG legen konkrete Anforderungen an ein Löschkonzept wie Löschfristen und Abläufe fest. Eine allgemeingültige und exakte Festlegung von Löschfristen für jeden Einzelfall ist nicht möglich, da diese von den einschlägigen datenschutzrechtlichen Vorschriften und den Verarbeitungszwecken abhängen.[105] Im Folgenden sollen die Kriterien zur Ableitung der entsprechenden Prozesse und Fristen und somit die Möglichkeiten geeigneter Löschkonzepte dargestellt werden.

3.1.2 Mögliche Vorgehensweisen zur Erarbeitung von Löschkonzepten

Sowohl zur Erfüllung der Löschbegehren betroffener Personen als auch bei der systematisch durch gesetzliche Vorgaben eintretenden Löschpflicht ist ein Löschkonzept also rechtlich und für die praktische Umsetzbarkeit unausweichlich. Wie den Experteninterviews zu entnehmen ist, überwiegt in der betrieblichen Praxis der Anteil der systematischen Löschpflicht unabhängig von einem Antrag der betroffenen Personen. Dabei erfordern beide Varianten zum Teil ähnliche Vorgehensweisen. Ein Löschkonzept ist ein Vorgang, bei dem personenbezogene Daten identifiziert und kategorisiert werden. Anschließend werden Kriterien zur Feststellung der Zweckerfüllung und Aufbewahrungsfristen festgelegt.[106] An diesem Prozess sind üblicherweise Datenschutz- und IT-Experten sowie Mitarbeiter des jeweils betroffenen Fachbereiches beteiligt. Das Rechte- und Rollenkonzept und die Umsetzung der weiteren Betroffenenrechte sollten dabei mit dem Löschkonzept in Einklang gebracht werden.[107] Um ein geeignetes Löschkonzept zu erarbeiten, sind verschiedene Ansätze denkbar, die im Folgenden näher erläutert werden.

---

[101] Vgl. *Jung, Alexander*: „Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO“, Zeitschrift für Datenschutz, 05/2018, S. 211.
[102] Vgl. *ebd.*
[103] Vgl. *Berning, Wilhelm; Keppeler, Lutz Martin*: „Technische und rechtliche Probleme bei der Umsetzung der DS-GVO Löschpflichten“, in: Zeitschrift für Datenschutz, 07/2017, S. 317.
[104] Vgl. *Wichtermann, Marco*: Einführung eines Datenschutz-Management-Systems im Unternehmen – Pflicht oder Kür? Kurzüberblick über die Erweiterungen durch die DS-GVO, in: Zeitschrift für Datenschutz, 09/2016, S. 422.
[105] Vgl. *Hammer, Volker*: DIN 66398 - Die Leitlinie Löschkonzept als Norm, in: Datenschutz und Datensicherheit, 08/2016, S. 529.
[106] Vgl. *Anke, Jürgen*, in: Knoll, Mathias; Strahringer, Susanne (Hrsg.): IT-GRC-Management – Governance, Risk und Compliance Grundlagen und Anwendungen, 1. Aufl., Springer, Wiesbaden 2017, S. 180.
[107] Vgl. *Koglin, Olaf,* in: Lachenmann, Matthias; Koreng, Ansgar (Hrsg.): Formularhandbuch Datenschutzrecht, 2.Aufl., C.H. Beck, München 2018, D.IV. Löschkonzepte Rn. 1 ff.

3.1.2.1 Löschkonzept nach DIN 66398

Der Betreiber eines deutschen Mautsystems sollte vor dem Start dieses Systems ein unternehmensweites Löschkonzept etablieren. Nach langjährigen, sehr positiven Erfahrungen wurde das Deutsche Institut für Normung darauf aufmerksam und eine unternehmensübergreifende Anwendbarkeit wurde geprüft. Infolgedessen entschloss sich ein Zusammenschluss mehrerer Unternehmen sowie dem Bundesministerium für Wirtschaft und Technologie zur Förderung eines Normprojekts, was am 08.04.2016 letztlich in der Veröffentlichung der „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“ als DIN 66398 mündete.[108] Mit der Norm soll den Unternehmen eine Orientierungshilfe für die Entwicklung und Etablierung eines Löschkonzepts zur Verfügung gestellt werden. Sie definiert Anwendungsbereiche, Begriffe und Abkürzungen, verschafft einen Überblick über das Vorgehen und gibt Hinweise zu den rechtlichen Vorgaben. Zusätzlich wird beschrieben, wie Datenkategorien und Löschfristen festgelegt werden, wie Löschklassen entstehen und die Kategorien darin eingeordnet werden. Abschließend werden Umsetzungsvorgaben erläutert und die Verantwortlichkeiten und Prozesse bestimmt, um eine beständige Funktion zu gewährleisten. Die Norm soll dabei kein allgemeingültiges Löschkonzept darstellen, sondern die Rahmenbedingungen zur Erstellung eines solchen aufzeigen und die Umsetzung der Anforderungen erleichtern. Ein Löschkonzept wird innerhalb dieses Ansatzes als „Festlegungen, mit denen eine verantwortliche Stelle sicherstellt, dass ihre personenbezogenen Datenbestände rechtskonform gelöscht werden“ beschrieben. Bei der Erarbeitung eines Löschkonzepts nach DIN 66398 wird in zwei Schritten vorgegangen. Zunächst muss für jede innerhalb der Norm sogenannte Datenart eine Löschregel festgelegt werden. Eine Datenart ist laut eigener Definition eine „Gruppe von Datenobjekten, die zu einem einheitlichen fachlichen Zweck verarbeitet wird“. Eine Löschregel wird als „Kombination aus Löschfrist und Bedingung für den Startzeitpunkt des Fristlaufs“ charakterisiert.[109] Im Rahmen der Klassifizierung von Datenarten ist der „einheitliche fachliche Zweck“ hervorzuheben, da sich für unterschiedliche Zwecke unterschiedliche Regeln und Vorgaben ergeben können. Hierbei kommt es nicht auf den Speicherort der Daten an. Die unterschiedlichen Datenarten resultieren also aus:

- den verschiedenen rechtlichen Vorgaben,
- dem Bezug auf verschiedene betroffene Personen,
- der Rechtsgrundlage der Erhebung und den damit verbundenen, möglicherweise unterschiedlichen Zwecken und
- der Verwendung der Daten in eigenständigen Teilprozessen.

In der Praxis sollten also personenbezogene Daten mit gleichen Rechtsvorgaben wie z.B. gleichen Aufbewahrungsfristen zusammengefasst werden. Ein gleicher Verwendungszweck ist ein weiterer Anhaltspunkt eine Datenart zu bilden, da die Daten somit gleichzeitig zu löschen sind. Um die Komplexität weiter zu verringern, ist es oft sinnvoll, Daten mit identischen Löschregeln fachlich zu unterteilen und entsprechend verschiedene Datenarten zu bilden. Dadurch können die Prozesse und die Kommunikation vereinfacht werden. Dasselbe gilt für Gruppen betroffener Personen, wie Mitarbeiter oder Kunden, unter denen beispielsweise deren Stammdaten aufgeteilt werden können. Besondere Arten personenbezogener Daten wie etwa Gesundheitsdaten sind mit einer speziellen Vertraulichkeit zu behandeln. Ein Zu-

[108] Vgl. *Hammer, Volker*: DIN 66398 - Die Leitlinie Löschkonzept als Norm, in: Datenschutz und Datensicherheit, 08/2016, S. 528 f.
[109] Vgl. *Deutsches Institut für Normung e.V. (Hrsg.)*: DIN 66398, Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Beuth Verlag, Berlin 2016, S. 11.

sammenlegen von Daten gleichgearteter Vertraulichkeitsstufen in einer Datenart erleichtert die spätere Umsetzung der Löschung enorm.[110] Ebenso unterscheidet sich beispielsweise der Fristbeginn je nach einschlägiger Aufbewahrungspflicht, was ein Zusammenfassen nach diesem Aspekt ebenso sinnvoll erscheinen lässt.[111] Alle personenbezogenen Daten eines Unternehmens werden dadurch zunächst kategorisiert. Im Anschluss wird jeder dieser Kategorien eine Frist sowie ein Startzeitpunkt der Frist zugeordnet und damit eine Löschregel erstellt. In diesem zweiten Schritt wird damit die datenschutzrechtlich vertretbare Löschfrist bestimmt, d.h. diese Frist stellt die längste Frist zur Löschung der personenbezogenen Daten dar. Die Fristen werden von der Norm als Vorhaltefrist und Regellöschfrist bezeichnet. Definiert wird die Vorhaltefrist dabei als „Frist, für die eine Datenart zur Verwendung in der verantwortlichen Stelle verfügbar sein muss“, was abhängig von den Zwecken der Verarbeitung und den gesetzlichen Aufbewahrungspflichten aus Regelwerken wie beispielsweise dem Handelsgesetzbuch (HGB) oder der Abgabenordnung (AO) ist. Die Regellöschfrist beschreibt hingegen die Frist, „nach der eine Datenart bei regulärer Verwendung in den Prozessen der verantwortlichen Stelle spätestens zu löschen ist“. Der über die Vorhaltefrist hinausgehende Zeitraum muss von dem Verantwortlichen eingeschätzt und datenschutzrechtlich verantwortet werden können. Je nach gesetzlichen Anforderungen können beide Fristen auch gleich lang sein. Somit ergibt sich die Regellöschfrist aus der Summe der Vorhaltefrist und der datenschutzrechtlich vertretbaren Frist im Hinblick auf die Gestaltung der Löschprozesse im jeweiligen Unternehmen.[112]

Der Beginn der Vorhaltefrist und der Regellöschfrist geht mit der Bestellung und deren Annahme, also mit dem Vertragsschluss, einher. Die Verwendung der verantwortlichen Stelle endet mit dem Zahlungseingang der Forderung. Darüber hinaus werden die Daten aufgrund entsprechender Aufbewahrungsfristen exemplarisch aus der AO oder dem HGB eine gewisse Zeit aufbewahrt. Damit endet die Vorhaltefrist, da die personenbezogenen Daten nicht mehr für die verantwortliche Stelle verfügbar sein müssen. Durch die Differenz zwischen der Vorhaltefrist und der Regellöschfrist soll der praktischen Umsetzung des Löschkonzepts in den Prozessen der Unternehmen Rechnung getragen werden. Jedoch sollte in der Zwischenzeit zumindest kein Zugriff der Anwender auf die Daten mehr möglich sein. Eine wichtige Rolle spielt in dem Zusammenhang auch die Differenzierung zwischen Archiven, Sicherungskopien und gesperrten Daten. In Archiven werden Daten aus rechtlichen Gründen über einen längeren Zeitraum aufbewahrt und es werden keine Änderungen mehr vorgenommen. Dabei können unterschiedliche Datenarten mit unterschiedlichen Löschfristen vorkommen. Sicherungskopien hingegen dienen der Wiederherstellung von Daten und enthalten meist mehrere Versionen mit unterschiedlich alten Daten derselben Art. Die Löschfrist der Daten tritt dadurch zu sehr unterschiedlichen Zeitpunkten ein. In Archiven müssen die personenbezogenen Daten also nach den jeweils festgelegten Löschregeln gelöscht werden, während für die gemischten Daten in den Sicherungskopien eigene verhältnismäßige Fristen bestimmt werden müssen. Gegebenenfalls müssen verschiedenen Datenarten in verschiedene Sicherungskopien aufgenommen werden. Um ein funktionierendes Wiederherstellungskonzept zu etablieren müssen die Löschfristen zwangsläufig über die Regellöschfristen hinausgehen, was zu einem Zielkonflikt führt. Die Überschreitung der Frist muss zwingend datenschutzrechtlich vertretbar sein. Für personenbezogene Daten, die nicht mehr für die Unternehmensprozesse an sich sondern lediglich zu Dokumentationszwecken gespeichert werden,

[110] Vgl. *Deutsches Institut für Normung e.V. (Hrsg.)*: DIN 66398, Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Beuth Verlag, Berlin 2016, S. 11.
[111] Vgl. *ebd.,* S. 21 ff.
[112] Vgl. *ebd.,* S. 17 ff.

müssen gegebenenfalls Zugriffsbeschränkungen umgesetzt werden. Zugriff dürfen lediglich noch die Mitarbeiter haben, die für die verbleibendem Aufgaben benötigt werden.[113]

In Form von sogenannten Löschklassen lassen sich anhand der jeweiligen Rechtsvorschriften Standardlöschfristen sowie standardisierte Startzeitpunkte zur Orientierung und einfacheren Definition der Fristen festlegen.[114] Durch die Kombination und die Einordnung der verschiedenen Datenarten, entstehen einzelne Löschklassen. Mit diesem Instrument kann ein einheitlicher Überblick für einen effizienten Prozess geschaffen werden. Im Rahmen der DIN 66398 wird eine solche Matrix folgendermaßen am Beispiel des Mautsystembetreibers Toll Collect GmbH dargestellt:

Startzeitpunkte	Standardfristen							
		Sofort	42 Tage	120 Tage	1 Jahr	4 Jahre	7 Jahre	12 Jahre
	Ab Erhebung			Mautdaten	Mautdaten mit besonderem Analysebedarf			
	Ab Ende Vorgang	Mautdaten nicht Mautpflichtiger Fahrzeuge, Weblogs	Kurzzeit-Doku., Betriebslogs	Einzelfahrtennachweis, voll erstattete Reklamationen	Vorgänge ohne Dokupflicht	Reklamations- und Forderungsdaten	Handelsbriefe	Buchhaltungsdaten
	Ab Ende Beziehung				ergänzende Stammdaten		Verträge	Kernstammdaten

Legende: Grün = Frist aus allgemeinen Gesetzen abgeleitet, Aubergine = Frist aus Spezialgesetzen abgeleitet, Blau = Frist frei gewählt

Abb. 1: Beispielhafte Matrix von Löschklassen[115]

Die Werte der beiden Achsen können wie nachfolgend erläutert definiert werden. Zunächst werden durch die Standardlöschfristen ähnlich lange Löschfristen zusammengefasst. Dadurch können die Datenarten den Löschklassen unkompliziert zugeordnet und die einschlägigen Fristen einfacher identifiziert werden. Hierbei wird bei dem Verfahren nach der DIN 66398 in drei Schritten vorgegangen:

[113] Vgl. *Deutsches Institut für Normung e.V. (Hrsg.)*: DIN 66398, Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Beuth Verlag, Berlin 2016, S. 17 ff.
[114] Vgl. Scheja, Gregor; Quae, Simon; Conrad, Isabell; Hausen, Dominik, in: Forgó, Nikolaus; Helfrich, Marcus; Schneider, Jochen (Hrsg.): Betrieblicher Datenschutz. Rechtshandbuch, 3. Aufl., C.H. Beck, München 2019, Teil IV. Kapitel 2. Technische und organisatorische Maßnahmen Rn. 30.
[115] Vgl. Deutsches Institut für Normung e.V. (Hrsg.): DIN 66398, Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Beuth Verlag, Berlin 2016, S. 30.

Schritt 1:

Im ersten Schritt werden Löschfristen für diejenigen Datenarten festgelegt, für die sie sich unmittelbar aus den Rechtsvorschriften ergeben. Der erste Schritt ist im Verhältnis zu den anderen trivial, da die Fristen direkt aus den Vorschriften übernommen werden können und damit bereits ein erheblicher Teil der identifizierten Datenarten abgedeckt wird. Ein klassisches Beispiel ist die Aufbewahrungsfrist von 10 Jahren für Buchhaltungsdaten gemäß § 147 AO und 257 HGB. Die ermittelten Fristen müssen danach unter Beachtung gleichartiger Längen zusammengefasst werden, um möglichst wenige, jedoch so viele Standardlöschfristen, wie datenschutzrechtlich nötig, zu erhalten.

Schritt 2:

Für spezielle Fälle, wie bei besonderen Kategorien personenbezogener Daten oder gesetzlich engen, aber unbestimmten Fristen ist ein weiter Schritt vonnöten. Hierfür muss eine Analyse der Dauer der Prozesse durchgeführt werden, für die die Daten verwendet werden und eine Auslegung der Rechtsvorschriften für die entsprechenden Fälle erfolgen. Aus diesem Schritt ergeben sich ergänzend zu Schritt 1 weitere Standardlöschfristen.

Schritt 3:

Zwischen den definierten Standardfristen können sich große Abstände ergeben, d.h. es können Situationen entstehen, bei denen der Zuordnung einer früheren Frist beispielsweise der Verarbeitungszweck entgegensteht, während die nächste größere Frist als datenschutzrechtlich nicht mehr vertretbar angesehen werden müsste. In solchen Ausnahmefällen können einzelne Fristen frei gewählt werden, allerdings besteht das Ziel darin, mit möglichst wenigen Standardlöschfristen zurechtzukommen. Üblicherweise ist die Festlegung anhand ausgewählter Datenarten stellvertretend für die Gesamtheit ausreichend.[116]

Zur Einordnung der Datenarten werden auf der zweiten Achse der Matrix die Startzeitpunkte benötigt. Die Startzeitpunkte werden von bestimmten Bedingungen während eines Prozesses abgeleitet. Dabei wird der Start des Fristenlaufs beim Eintritt folgender Bedingungen unterschieden:

- Erhebung der personenbezogenen Daten,
- Ende eines Vorgangs und
- Ende der Beziehung zum Betroffenen (Spezialfall der Bedingung „Ende eines Vorgangs“, da mit dieser Bedingung die Löschfrist für mehrere Datenarten gleichzeitig starten muss).[117]

Bei drei Startpunkten, wie im obigen Beispiel dargestellt, ergeben sich pro Standardlöschfrist drei Löschklassen, von denen nicht alle verwendet werden müssen. Je weniger Löschklassen belegt werden, desto mehr reduziert sich die Komplexität weiter. Die identifizierten Datenarten müssen nun in die dadurch festgelegten Löschklassen eingeteilt werden. Aus den Zwecken der Verarbeitung ergeben sich die Dauer der Verwendung sowie die Aufbewahrungsfristen und damit die Vorhaltefrist anhand derer die Löschklassen zugeordnet werden können. In Kombination mit dem entsprechenden Startzeitpunkt wird die Standardlöschfrist gewählt, die der Vorhaltefrist entspricht oder nur unwesentlich größer ist. Eine Differenz

[116] Vgl. *Hammer, Volker*: DIN 66398 - Die Leitlinie Löschkonzept als Norm, in: Datenschutz und Datensicherheit, 08/2016, S. 529 f.
[117] Vgl. *Deutsches Institut für Normung e.V. (Hrsg.)*: DIN 66398, Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Beuth Verlag, Berlin 2016, S. 29 f.

zwischen der Standardlöschfrist und der Vorhaltefrist muss datenschutzrechtlich vertretbar sein. Ist dies nicht möglich, muss eine andere Löschklasse gewählt werden. Häufig ist bei näherer Betrachtung eine kürzere Vorhaltefrist möglich, anderenfalls kann durch weiteres Unterteilen der Datenart eine passende Einordnung erreicht werden. Sollte noch immer keine geeignete Klassifizierung gefunden werden, muss eine weitere Standardlöschfrist oder eine spezifische Frist für diesen Einzelfall definiert werden. Durch diese Einordnung und die gegebenenfalls datenschutzrechtlich vertretbaren Differenzen entstehen die Regellöschfristen. Die entsprechende Datenart ist bei regulärer Verwendung in den Prozessen der verantwortlichen Stelle folglich spätestens nach Ablauf dieser Frist zu löschen. Die Löschregeln werden im Anschluss in einem Dokument „Regellöschfristen“ für die, an dem Prozess Beteiligten ausformuliert. Die Startzeitpunkte werden dabei konkretisiert, d.h. aus „Ende Vorgang“ wird je nach Art des Vorgangs im Unternehmen dann z.B. „Zeitpunkt des Vertragsschlusses“, um ein besseres Verständnis der beteiligten Personen zu erreichen. Zusätzlich werden die Standardlöschfristen in Regellöschfristen übertragen.[118]

Bisher wurden die Löschregeln im ersten Teil des Löschkonzepts technikunabhängig festgelegt. Daraus müssen nun Umsetzungsvorgaben abgeleitet werden, um die Löschung in allen Systemen und Prozessen zuverlässig durchsetzen zu können. Die Prozesse werden dabei in Querschnittsbereiche, Einzelsysteme, manuelle Prozesse und Auftragnehmer aufgeschlüsselt. Querschnittsbereiche können Backups oder Log-Protokolle sein, für die die Vorgaben oft einheitlich geregelt werden können. In diesem Bereich wird eine Umsetzung über Unternehmensrichtlinien empfohlen. Für IT-Systeme, die nicht von den Querschnittsbereichen erfasst wurden, müssen eigene Umsetzungsvorgaben entwickelt werden, um die personenbezogenen Daten auch in den konkret betroffenen Systemen zu löschen. Dies kann über individuelle Konzepte oder durch System- bzw. Betriebshandbücher erfolgen. Dadurch wird bereits der überwiegende Teil der relevanten Daten abgedeckt, allerdings müssen auch die Bestände in manuellen Prozessen berücksichtigt werden. Entsprechende Vorgaben sollen durch Arbeitsanweisungen an die beteiligten Personen übermittelt werden. Von großer Relevanz ist auch das Sicherstellen der Einhaltung der Löschfristen bei Auftragnehmern. Anhand vertraglicher Vereinbarungen müssen entsprechende Weisungen erteilt und die Umsetzungsvorgaben durchgesetzt werden. Das Speichern über die volle Regellöschfrist ist häufig nicht in allen IT-Systemen notwendig. Durch ein früheres Löschen in den entsprechenden Systemen wird der Datenschutzgrundsatz der Datensparsamkeit berücksichtigt und umgesetzt. Für Restbestände in IT-Systemen, die aufgrund von Fehlern in den Löschabläufen oder aus anderen Gründen nicht von den Regelprozessen erfasst wurden, sollten in dem Löschkonzept Verantwortlichkeiten zur Identifikation und Löschung festgelegt werden.[119] Selbstredend entstehen in bestimmten Situationen auch Ausnahmen, in denen von der Regellöschfrist abgewichen werden muss. Wenn Daten beispielsweise aufgrund eines Rechtsstreits länger aufbewahrt werden müssen, kann hierfür eine neue Datenart gebildet und die benötigten Daten gekennzeichnet werden um vorübergehend von der Löschung ausgeschlossen zu sein. Bei IT-Störungen oder sonstigen Fehlern in den Beständen können die Einzelfälle über das Change-Management gesteuert werden.[120] Die folgenden Situationen werden ausdrücklich nicht von der Norm erfasst:

[118] Vgl. *Hammer, Volker*: DIN 66398 - Die Leitlinie Löschkonzept als Norm, in: Datenschutz und Datensicherheit, 08/2016, S. 531.
[119] Vgl. *Deutsches Institut für Normung e.V. (Hrsg.)*: DIN 66398, Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Beuth Verlag, Berlin 2016, S. 34 ff.
[120] Vgl. *Hammer, Volker*: DIN 66398 - Die Leitlinie Löschkonzept als Norm, in: Datenschutz und Datensicherheit, 08/2016, S. 532.

- Das Löschen von unberechtigt erhobenen personenbezogenen Daten,
- das Löschen von personenbezogenen Daten nach einem berechtigten Löschbegehren des Betroffenen und
- das Löschen von personenbezogenen Daten beim Rückbau von Systemen.[121]

Für diese Fälle ist die Leitlinie also nicht hilfreich und eine zusätzliche Lösung muss entwickelt werden.

Nach Festlegung der Abläufe und Verantwortlichkeiten stellt sich die wichtige Frage nach den Kriterien zur Umsetzung einer Löschung i.S.d. Gesetzes. Aus den Experteninterviews konnten Schwierigkeiten bezüglich des Löschbegriffs und dessen Anforderungen an eine gesetzeskonforme Umsetzung einer Löschung erkannt werden. Löschen bedeutet im Kontext der Norm „behandeln von personenbezogenen Daten derart, dass sie nach dem Vorgang nicht mehr vorhanden oder unkenntlich sind und nicht mehr verwendet oder rekonstruiert werden können“. Dies kann bejaht werden, sofern eine Wiederherstellung nicht mehr oder nur mit unverhältnismäßig großem Aufwand möglich ist. In rechtlich genehmigten Ausnahmefällen können personenbezogene Daten auch lediglich anonymisiert werden, was als „Prozess, durch den personenbezogene Daten so verändert werden, dass der Betroffene nicht mehr direkt oder indirekt identifiziert werden kann“ beschrieben wird. Für eine Anonymisierung werden nur die Daten gelöscht, die eine Zuordnung ermöglichen.[122] Bei der Wahl der Mittel zur Anonymisierung müssen alle Mittel berücksichtigt werden, die der Verantwortliche oder eine andere Person nach allgemeinem Ermessen wahrscheinlich nutzen werden und dabei ist gleichzeitig auf die Kosten und den Zeitaufwand abzustellen.[123]

Das Löschkonzept muss ständig anhand der Unternehmensentwicklungen sowie der rechtlichen Entwicklungen fortgeschrieben und angepasst werden. Dafür müssen Verantwortlichkeiten, Informationspflichten und Freigabebeteiligungen festgelegt werden. Um die gesetzlichen Verpflichtungen einhalten und das Konzept gemäß der DIN 66398 umsetzen zu können müssen die genannten Punkte und alle, für die Durchführung der Prozesse notwendigen Regelungen in einer Aufbau- und Ablauforganisation bestimmt werden. Für die gesamte Umsetzung ist die Geschäftsleitung verantwortlich.[124]

3.1.2.2 Löschkonzept nach Olaf Koglin

Eine weitere mögliche Vorgehensweise beschreibt Olaf Koglin, der dabei viel Wert auf ein Rechte- und Rollenkonzept, Identity/Access Management und die Umsetzung der weiteren Rechte der Betroffenen i.S.d. Art. 15 ff. DSGVO legt. Durch die Einbindung in möglichst viele verwandte Themen sollen Synergien geschaffen werden. Dieses Löschkonzept umfasst die folgenden Schritte:

1. Schritt:

Zunächst muss der Scope des Löschkonzepts in Form einer Abwägung zwischen vollständiger Compliance und einem risikoorientierten Ansatz festgelegt werden. Grundsätzlich sollte eine umfangreiche und vollständige Löschung erfolgen, da es in der Praxis jedoch Situatio-

[121] Vgl. *Deutsches Institut für Normung e.V. (Hrsg.)*: DIN 66398, Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Beuth Verlag, Berlin 2016, S. 20.
[122] Vgl. ebd., S. 10.
[123] Vgl. *Klar, Manuel; Kühling, Jürgen,* in: Buchner, Benedikt; Kühling, Jürgen (Hrsg.): Datenschutz-Grundverordnung/BDSG, 2. Aufl., C.H. Beck, München 2018, Art. 4 Nr. 1 Rn. 31 ff.
[124] Vgl. *Deutsches Institut für Normung e.V. (Hrsg.)*: DIN 66398, Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Beuth Verlag, Berlin 2016, S. 44.

nen gibt, in denen beispielsweise lediglich ein User selbst auf die personenbezogenen Daten zugreifen kann, ist ein pragmatisches und zweckmäßiges Vorgehen häufig der zu bevorzugende Weg. Bei der Abwägung soll sich an den Risiken durch Bußgelder, Imageschäden und Abmahnungen orientiert werden. Im Zuge dessen sollte die Fokussierung der Aufsichtsbehörden verfolgt und berücksichtigt werden.[125]

2. Schritt

Im zweiten Schritt müssen die Lösch- und Aufbewahrungsinteressen ebenfalls abgewogen werden. Zu diesem Zweck wird eine allgemeine Übersicht über die Aufbewahrungsfristen erstellt. Durch diese Übersicht können die entsprechenden Daten im weiteren Verlauf einfacher und schneller den jeweiligen Fristen zugeordnet werden. Jedoch können die Aufbewahrungsfristen, wie bereits in Kapitel 3.1.2.1 näher beschrieben, oftmals aufgrund von Rechtsstreitigkeiten oder anderen Ausnahmen über diese allgemeinen Standardfristen hinausgehen und es tritt nicht direkt nach Ablauf der allgemeinen Fristen die Löschpflicht ein. Auf der anderen Seite kann hier bei bestimmten Datenkategorien schon vor Ablauf der Frist eine Pseudonymisierung oder eine Anonymisierung möglich sein. Bei einer Pseudonymisierung müssen alle Merkmale, die einen Personenbezug herstellen durch einen anderen Wert oder einen Code ersetzt werden, sodass die Informationen den betroffenen Personen ohne das Hinzuziehen zusätzlicher Informationen nicht mehr zugeordnet werden können.[126] Die Pseudonymisierung wird an vielen Stellen der DS-GVO als geeignetes Mittel z. B. zum Schutz der Rechte und Freiheiten betroffener Personen genannt.[127] Der Vorteil der Pseudonymisierung liegt daher zum einen in der damit einhergehenden Anwendung von TOMs und zum anderen in den positiven Auswirkungen auf eine mögliche Interessenabwägung.[128] Pseudonyme Daten gemäß Art. 4 Nr. 5 DS-GVO sind dennoch weiterhin personenbezogene Daten und als solche zu behandeln. Von einer Anonymisierung kann, wie in Kapitel 3.1.2.1 näher ausgeführt, ausgegangen werden, wenn die Wiederherstellung nicht mehr oder nur mit unverhältnismäßig großem Aufwand möglich ist. Da die Zuordnung der Fristen zu den verschiedenen Datenkategorien nicht ausschließlich rechtliche Komponenten beinhaltet, muss die Abwägung unter Einbeziehung der Beteiligten aus Geschäftsleitung, Fachbereich und IT erfolgen. Der Einschränkung der Verarbeitung gemäß Art. 18 DS-GVO wird bei diesem Löschkonzept keine große Bedeutung zugeschrieben, da durch diese Aktion zu einem früheren Zeitpunkt keine Privilegierung diesbezüglich entsteht. Jedoch haben betroffene Personen gemäß Art. 18 Abs. 1 DS-GVO in den dort geregelten Fällen das Recht, die Einschränkung der Verarbeitung zu verlangen. Diese Möglichkeit muss gleichwohl immer in Betracht gezogen und umgesetzt werden können.[129]

3. Schritt

Nach den Abwägungen und dem damit feststehenden Scope sowie den bestimmten Löschfristen, müssen Datenkategorien gebildet und anhand der Verarbeitungszwecke und Aufbe-

[125] Vgl. *Koglin, Olaf,* in: Lachenmann, Matthias; Koreng, Ansgar (Hrsg.): Formularhandbuch Datenschutzrecht, 2.Aufl., C.H. Beck, München 2018, D.IV. Löschkonzepte Rn. 1 ff.
[126] Vgl. *Schwartmann, Rolf; Mühlenbeck, Robin L.,* in: Schwartmann, Rolf; Jaspers, Andreas; Thüsing, Gregor; Kugelmann, Dieter (Hrsg.): DS-GVO/BDSG. Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, C.F. Müller, Heidelberg 2018, Art. 4 Nr. 5 Rn. 62 f.
[127] Vgl. *Roßnagel, Alexander*: „Pseudonymisierung personenbezogener Daten. Ein zentrales Instrument im Datenschutz nach der DS-GVO“, in: Zeitschrift für Datenschutz, 06/2018, S. 243.
[128] Vgl. *Herfurth, Constantin*: „Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO“, in: Zeitschrift für Datenschutz, 11/2018, S. 516.
[129] Vgl. *Koglin, Olaf,* in: Lachenmann, Matthias; Koreng, Ansgar (Hrsg.): Formularhandbuch Datenschutzrecht, 2.Aufl., C.H. Beck, München 2018, D.IV. Löschkonzepte Rn. 1 ff.

wahrungsfristen den entsprechenden Löschfristen zugeordnet werden. Die Fristen müssen derart konkret formuliert werden, damit die Umsetzung durch die Mitarbeiter und die Konfiguration der automatisierten Löschung durch die IT in Standardfällen keine Nachfragen erzeugt. Die Vorgaben müssen also so klar und deutlich konzipiert sein, dass jeder einzelne Mitarbeiter versteht, wann die Daten welcher Datenkategorie gelöscht werden müssen.[130]

4. Schritt

Im Anschluss an die Zuordnung der Fristen zu den Datenkategorien, müssen die Verantwortlichkeiten für die Löschung und die Einschränkung der Verarbeitung festgelegt werden. Für jede Datenkategorie wird entweder die Zuständigkeit durch die IT-Abteilung oder die jeweilige Fachabteilung bestimmt. Wichtig dabei ist, keine Einzelpersonen zu bestimmen, sondern deren Rollen bzw. Positionen und einen Vertreter. Anders als bei der Vorgehensweise gemäß der DIN 66398 erfolgt hier keine Aufteilung nach Prozessen und Anweisung in unterschiedlichen Formen wie Richtlinien oder Betriebshandbücher, sondern eine direkte Zuteilung und Anweisung der zuvor definierten Löschvorgaben an die Verantwortlichen.[131]

5. Schritt

Das Löschkonzept sollte mit den folgenden verwandten Themen in Einklang gebracht werden:

- Löschanträge durch betroffene Personen gemäß Art. 17 Abs. 1 DS-GVO müssen einzeln und eng mit dem entwickelten Löschkonzept abgestimmt werden, da diese nicht durch die festgelegten Löschregeln abgedeckt werden. In der Praxis betrifft dieses Verlangen zwar nur den geringeren Teil der Löschung, jedoch muss der Regelung die identische Wichtigkeit zugeschrieben werden.
- Im Rahmen der Umsetzung der weiteren Rechte der Betroffenen wie z.B. dem Auskunftsrecht, dem Recht auf Berichtigung oder dem Recht auf Einschränkung der Verarbeitung gemäß Art. 15 ff. DS-GVO können Synergien entstehen. Um die Abläufe zu optimieren und alle Betroffenenrechte vollumfänglich durchsetzen zu können, ist das Ineinandergreifen der Mechanismen von enormer Bedeutung.
- Durch ein Rechte- und Rollenkonzept muss der Zugriff auf die personenbezogenen Daten geregelt werden. Bei Personaländerungen müssen durch ein Identity and Access Management automatisch Zugriffsrechte und sonstige diesbezügliche Berechtigungen entzogen bzw. geändert werden.
- Informationssicherheitskonzepte, welche den Umgang mit nicht personenbezogenen Daten regeln, können ebenfalls von den in dem Löschkonzept definierten Vorgehensweisen profitieren.
- Neben den rechtlichen Aspekten müssen auch die technischen Komponenten berücksichtigt werden, um eine tatsächliche Löschung i.S.d. Gesetzes erreichen zu können. Die Anforderungen an eine gesetzeskonforme Löschung wurden unter Kapitel 3.1 ausgeführt.
- Das Vorliegen und die Dokumentation der Zwecke der Verarbeitung ist wesentlich für die Bestimmung der Speicher- bzw. Löschfristen.[132]

[130] Vgl. *Koglin, Olaf,* in: Lachenmann, Matthias; Koreng, Ansgar (Hrsg.): Formularhandbuch Datenschutzrecht, 2.Aufl., C.H. Beck, München 2018, D.IV. Löschkonzepte Rn. 1 ff.
[131] Vgl. *ebd.*
[132] Vgl. *Koglin, Olaf,* in: Lachenmann, Matthias; Koreng, Ansgar (Hrsg.): Formularhandbuch Datenschutzrecht, 2.Aufl., C.H. Beck, München 2018, D.IV. Löschkonzepte Rn. 1 ff.

6. Schritt

Um den Anforderungen an die Datenschutz-Compliance bei dieser Vorgehensweise gerecht zu werden, wird empfohlen, auf Standards zu Compliance Management Systemen wie dem IDW PS 980 zurückzugreifen.[133] Das Institut der deutschen Wirtschaftsprüfer hat Prüfungsstandards unter anderem für Compliance Management Systeme entwickelt. Viele Compliance-Bereiche sind im Zuge der Jahresabschlussprüfung von Wirtschaftsprüfern zu prüfen. Der IDW PS 980 hat zwar wie alle IDW Prüfungsstandards keine Gesetzeskraft, jedoch enthält er anerkannte Best Practices zur Umsetzung eines Compliance Management Systems und damit auch zu den datenschutzrechtlichen Pflichten.[134] Diese Vorgaben können der Erleichterung der Umsetzung und Einbindung des Löschkonzepts in ein funktionierendes Compliance Management System dienen.

3.1.2.3 Löschkonzept nach Wilhelm Berning

Einen umsetzungs- und technikbezogenen Ansatz beschreibt Wilhelm Berning, jedoch bildet auch hier die Festlegung bestimmter Kriterien wie Datencluster und Aufbewahrungsfristen die Grundlage des Löschkonzepts. Zusätzlich, zu den üblicherweise beteiligten Personen aus den Fachabteilungen, dem Datenschutz- und IT-Bereich, wird hier empfohlen, bei komplexen Prozessstrukturen und abhängig von der Organisation Prozessspezialisten einzubinden. Aufgrund des sehr technik- und IT-bezogenen Ansatzes, werden die Vorschriften der DS-GVO auch in diese Denkweise übersetzt. Übertragen auf die IT sind personenbezogene Daten i.S.d. Gesetztes „auf ein Individuum bezogene Einträge z.B. in einer Tabelle einer Datenbank“.[135] In der Regel liegen mehrere Datenbanken vor, bei denen für jede ein separates Löschkonzept erstellt werden muss. Aufgrund der sehr umfangreichen Datenstrukturen müssen die jeweiligen Datenbanken schon zu Beginn der Entwicklung entsprechend strukturiert werden und verschiedene Ablagen für personenbezogene und nicht personenbezogene Daten erstellt werden. Somit ist eine klare Erkennbarkeit der personenbezogenen Daten gegeben. Die Struktur sollte sich an den Geschäftsprozessen orientieren und den Zweck der Verarbeitung abbilden. In den Tabellen muss durch bestimmte Vermerke und Regeln berücksichtigt werden, dass einige personenbezogene Daten zu mehreren Zwecken verarbeitet werden, um die Daten zum richtigen Zeitpunkt zu löschen. Innerhalb der Datenbanken bestehen verschiedene Datensätze, die jeweils Datenfelder mit den personenbezogenen Daten enthalten. Für die Zuordnung ist eine eindeutige Bezeichnung wichtig. Für unterschiedliche Zwecke wie z.B. zur Zeitwirtschaft oder für die Personalentwicklung existieren somit unterschiedliche Tabellen, die wiederum personenbezogene Daten dieser Kategorie enthalten. In diesem Beispiel wären dies Daten unterschiedlicher Mitarbeitertypen von den Praktikanten bis zu den Angestellten. Somit können die Daten anhand dieser Beschreibungen leichter identifiziert werden. Je nach Möglichkeit werden Tabellen oder Datensätze in sogenannte Datencluster unterteilt. Datencluster stellen eine zu löschende Einheit dar und sind mit Datenkategorien vergleichbar. Im ersten Schritt werden hier also die Datencluster identifiziert, beschrieben und festgelegt. Nachfolgend werden den Clustern die Zwecke der Verarbeitung zugeordnet und die Kriterien der Zweckerfüllung festgelegt. In der Zeit zwischen der Zweckerfüllung und dem endgültigen Löschen, müssen die Zugriffsrechte auf die personenbezogenen Daten angepasst werden. In dieser Zwischenzeit werden die Daten nicht mehr in der ursprünglichen Form verarbeitet und nur noch z.B. aufgrund von Aufbewahrungspflichten

[133] Vgl. *ebd.*
[134] Vgl. *Koglin, Olaf,* in: Lachenmann, Matthias; Koreng, Ansgar (Hrsg.): Formularhandbuch Datenschutzrecht, 2.Aufl., C.H. Beck, München 2018, D.IV. Löschkonzepte Rn. 1 ff.
[135] Vgl. *Berning, Wilhelm; Meyer, Kyrill; Keppeler, Lutz M.*, in: Knoll, Mathias; Strahringer, Susanne (Hrsg.): IT-GRC-Management – Governance, Risk und Compliance Grundlagen und Anwendungen, 1. Aufl., Springer, Wiesbaden 2017, S. 188.

gespeichert, wodurch weitaus beschränktere Zugriffsrechte ausreichen dürften. Der jeweilige Fachbereich sollte möglichst messbare Kriterien der Zweckerfüllung beispielsweise in Form eines Datums festlegen. Die Definition der Aufbewahrungspflichten erfolgt in Abstimmung der Fachbereiche mit der juristischen Datenschutzexpertise. Um Mehrfachnutzungen identifizieren zu können, müssen die Datenfelder und somit die einzelnen Daten, pro Datencluster aufgeführt werden. Dadurch kann eine notwendige längere Aufbewahrung aufgrund anderer Zwecke oder Aufbewahrungspflichten erkannt werden. Für die IT-seitige Umsetzung dieses Löschkonzepts sind weitreichende Kenntnisse im Bereich von Datenbanken und Datenbank-Management-Systemen notwendig. Je nach eingesetztem Tool variiert der Aufwand bzw. die Umsetzbarkeit.[136]

3.2 AUFTRAGSVERARBEITUNG

3.2.1 Verpflichtung regelmäßiger Kontrollen technischer und organisatorischer Maßnahmen

Der hohe Kosten- und Effizienzdruck, sowohl in der Privatwirtschaft als auch in der öffentlichen Verwaltung, erfordert bei den Behörden und Unternehmen immer mehr eine Arbeitsteilung oder Outsourcing von bestimmten Prozessen.[137] Dadurch kann zusätzliches Spezialwissen von externen Stellen einbezogen und genutzt werden. Ebenso können fehlende personelle Kapazitäten aufgrund der gestiegenen rechtlichen Anforderungen und der ständigen technischen Fortschritte Gründe für eine solche Auslagerung sein.[138] Dies kommt häufig in Bereichen wie der Bearbeitung von Gehaltsabrechnungen, bei der Vernichtung von Dokumenten und Akten oder bei IT-Dienstleistungen zur Anwendung. Ein viel diskutierter und wichtiger Anwendungsfall ist dabei auch das Cloud Computing. Dabei wird beispielsweise Software, Speicherkapazität oder auch eine ganze IT-Infrastruktur extern zur Verfügung gestellt. Dadurch wird die Datenverarbeitung in die Cloud ausgelagert, die in Form von Rechnerlandschaften von externen Anbietern über das Internet bereitgestellt wird.[139] Bei Telekommunikationsdienstleistungen oder Postdienstleistungen, die in Spezialgesetzen geregelt werden, liegt hingegen ausdrücklich keine Auftragsverarbeitung vor.[140] Der Transfer personenbezogener Daten von einem Verantwortlichen an einen Dienstleister kann im Fall eines Auftragsverarbeitungsverhältnisses privilegiert sein. Die einschlägigen gesetzlichen Anforderungen für diese Konstellation sind insbesondere in Art. 28 DS-GVO geregelt. Damit wurde aus der Auftragsdatenverarbeitung nach § 11 BDSG a.F. nun die Auftragsverarbeitung gemäß der genannten Vorschrift. Die Regelungen aus § 62 BDSG zur Auftragsverarbeitung dürfen nicht mit denen nach Art. 28 DS-GVO gleichgestellt werden. Das Ziel der Vorschrift ist in Art. 1 Abs. 1 Richtlinie Justiz/Inneres EU 2016/680 beschrieben. Damit bezieht sich die Norm auf den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten

[136] Vgl. *Berning, Wilhelm; Meyer, Kyrill; Keppeler, Lutz M.*, in: Knoll, Mathias; Strahringer, Susanne (Hrsg.): IT-GRC-Management – Governance, Risk und Compliance Grundlagen und Anwendungen, 1. Aufl., Springer, Wiesbaden 2017, S. 187-193.
[137] Vgl. *Tinnefeld, Marie-Theres; Buchner, Benedikt; Petri, Thomas; Hof, Hans-Joachim*: Einführung in das Datenschutzrecht, 7. Aufl., De Gruyter, Oldenbourg 2020, S. 275 f.
[138] Vgl. *Der Bayerische Landesbeauftragte für den Datenschutz*: „Auftragsverarbeitung Orientierungshilfe“, URL: https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf, S. 5, Abruf: 16.10.2020.
[139] Vgl. *Tinnefeld, Marie-Theres; Buchner, Benedikt; Petri, Thomas; Hof, Hans-Joachim*: Einführung in das Datenschutzrecht, 7. Aufl., De Gruyter, Oldenbourg 2020, S. 275 f.
[140] Vgl. *Bitkom e. V.*: „Begleitende Hinweise zu der Anlage Auftragsverarbeitung – Leitfaden“, URL: https://www.bitkom.org/sites/default/files/file/import/170515-LF-Auftragsverarbeitung-online.pdf, S. 23, Abruf: 02.11.2020.

durch 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. § 62 BDSG fällt unter den dritten Teil des BDSG, wofür der Anwendungsbereich nochmals explizit auf zuständige öffentliche Stellen beschränkt wird.[141] Werden die nachfolgend erläuterten Voraussetzungen erfüllt, wird der Dienstleister und damit Auftragsverarbeiter nach Art. 4 Nr. 10 DS-GVO nicht weiter als sogenannter „Dritter" klassifiziert. Dadurch ist keine weitere Rechtsgrundlage für die Verarbeitung personenbezogener Daten gemäß Art. 6-10 DS-GVO für den Transfer der personenbezogenen Daten erforderlich.[142] Dabei ist zwischen den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" zu unterscheiden, welche in Art 4 Nr. 7, 8 DS-GVO definiert sind. Der Verantwortliche entscheidet demnach allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten. Ein Auftragsverarbeiter verarbeitet personenbezogene Daten gemäß diesem Artikel im Auftrag des Verantwortlichen. Die Art. 29 Datenschutzgruppe stellt in ihrem Working Paper 169 zwei wesentliche Bedingungen an einen Auftragsverarbeiter. Zum einen muss er eine rechtliche Eigenständigkeit besitzen und zum anderen muss die Verarbeitung der personenbezogenen Daten im Auftrag des Verantwortlichen erfolgen. Ein Handeln im Auftrag liegt demnach vor, wenn der Auftragsverarbeiter die erteilten Weisungen zumindest hinsichtlich des Zwecks der Verarbeitung und der wesentlichen Elemente der Mittel befolgt.[143] Der Grundgedanke liegt dabei in einer Einheit des Auftraggebers und des Auftragnehmers.[144] Gemäß Art. 29 DS-GVO handelt der Auftragsverarbeiter dem Verantwortlichen gegenüber weisungsgebunden, also ohne eigenen Wertungs- und Entscheidungsspielraum, wodurch er gemäß Art. 4 Nr. 10 DS-GVO eben nicht mehr als Dritter im Sinne des Gesetztes angesehen wird. Diese Vorschrift korrespondiert mit Art. 28 Abs. 3 S. 2 lit. a) DS-GVO, wodurch der Vertrag zwischen den Parteien diese Regelung enthalten muss. Der Auftragsverarbeiter verfolgt keine eigenen Interessen und kann als „verlängerter Arm" des Verantwortlichen gesehen werden.[145] Die einzig erlaubte Abweichung von den Weisungen sind Verpflichtungen durch das Recht der Union oder der Mitgliedstaaten, um den Auftragsverarbeiter von den Interessenskonflikten zwischen Vertragsstrafen und staatlichen Sanktionen zu entbinden. In Deutschland kann so ein Fall etwa bei polizeirechtlichen Bestimmungen zum Tragen kommen.[146] Im Zuge dessen muss im Vorlauf auch zwischen der Auftragsverarbeitung und gemeinsam für die Verarbeitung Verantwortlichen (Joint Controllership) nach Art. 26 DS-GVO unterschieden werden. Gemeinsam Verantwortliche legen die Zwecke und Mittel der Verarbeitung im Gegensatz zum Auftragsverarbeiter gemeinsam fest. Bei dieser Form muss in einer Vereinbarung klar geregelt werden wer welche Verpflichtungen der Verordnung wie die Rechte der Betroffenen erfüllt. Da es sich bei beiden Parteien um Verantwortliche handelt, benötigen im Gegensatz zu der

[141] Vgl. *Spoerr, Wolfgang*, in: Brink, Stefan; Wolff, Heinrich Amadeus (Hrsg.): BeckOK Datenschutzrecht, 33. Edition, C.H. Beck, München 2020, § 62 Rn. 3 f.
[142] Vgl. *Der Bayerische Landesbeauftragte für den Datenschutz*: „Auftragsverarbeitung Orientierungshilfe", URL: https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf, S. 7, Abruf: 20.10.2020.
[143] Vgl. *Art. 29 – Datenschutzgruppe*: „WP 169 Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf, S. 9 ff., Abruf: 22.10.2020.
[144] Vgl. *Tinnefeld, Marie-Theres; Buchner, Benedikt; Petri, Thomas; Hof, Hans-Joachim*: Einführung in das Datenschutzrecht, 7. Aufl., De Gruyter, Oldenbourg 2020, S. 276.
[145] Vgl. *Der Bayerische Landesbeauftragte für den Datenschutz*: „Auftragsverarbeitung Orientierungshilfe", URL: https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf, S. 12, Abruf: 20.10.2020.
[146] Vgl. *Petri, Thomas,* in: Simitis, Spiros; Hornung, Gerrit; Spiecker, Indra (Hrsg.): Datenschutzrecht. DSGVO mit BDSG, Nomos, Baden-Baden 2019, Art. 28 Rn. 59 ff.

Auftragsverarbeitung auch beide eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten.[147] Der Bayerische Landesbeauftragte für den Datenschutz stellt folgende Kriterien zur Abgrenzung zur Verfügung:

Für eine Auftragsverarbeitung spricht:

- „Der Dienstleister besitzt keine Entscheidungsbefugnis hinsichtlich des Zwecks der Verarbeitung personenbezogener Daten. Der Verantwortliche, der den Auftrag erteilt, behält die Hoheit über die Verwendung der Daten einschließlich deren Löschung oder Vernichtung.
- Der Dienstleister ist ausführlichen Weisungen des Verantwortlichen unterworfen, die ihm wenig Spielraum lassen.
- Die Daten werden dem Dienstleister von dem Verantwortlichen lediglich zur Verfügung gestellt.
- Der Vertrag enthält Weisungen bezüglich der Art der durchzuführenden Datenverarbeitung und des Umgangs mit den personenbezogenen Daten (welche Daten wie lange zu welchem Zweck verarbeitet werden, wer Zugang zu ihnen hat), gewährt dem Dienstleister aber keine eigenen Nutzungsrechte. Es besteht somit ein vertragliches Nutzungsverbot.
- Der Dienstleister hat im Außenverhältnis keinerlei Entscheidungsbefugnisse.
- Der Dienstleister wird durch den Verantwortlichen, der den Auftrag erteilt, überwacht.

Gegen eine Auftragsverarbeitung spricht:

- Der Dienstleister erhält das Recht zur Nutzung der personenbezogenen Daten zu eigenen Zwecken.
- Verantwortlicher und Dienstleister entscheiden gemeinsam über Zweck und wesentliche Elemente der Mittel der Datenverarbeitung.
- Die zugrunde liegende fachliche Aufgabe wird auf den Dienstleister übertragen.
- Der Verantwortliche besitzt keinen entscheidenden Einfluss auf die Datenverarbeitung durch den Dienstleister oder keine umfassenden Informationsrechte gegenüber dem Dienstleister.
- Der Dienstleister entscheidet auch selbst, auf welche Weise wann welche Daten verarbeitet werden.“[148]

Liegt eine Auftragsverarbeitung vor, wird dem Verantwortlichen in Art. 28 Abs. 1 DS-GVO eine Auswahlverantwortung auferlegt. Demnach muss er dafür bürgen, dass der Auftragsverarbeiter hinreichend Garantien dafür bietet, dass geeignete TOMs so durchführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der Verordnung erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Die Grundlage einer Auftragsverarbeitung ist ein individueller Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter, der den Auftragsverarbeiter bindet. Eine solche Vereinbarung ist ebenfalls in Form von Standardvertragsklauseln möglich, die von der EU-Kommission oder den

[147] Vgl. *Bitkom e. V.*: „Begleitende Hinweise zu der Anlage Auftragsverarbeitung – Leitfaden“, URL: https://www.bitkom.org/sites/default/files/file/import/170515-LF-Auftragsverarbeitung-online.pdf, S. 17, Abruf: 20.10.2020.
[148] *Der Bayerische Landesbeauftragte für den Datenschutz*: „Auftragsverarbeitung Orientierungshilfe“, URL: https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf, S. 12 f., Abruf: 21.10.2020.

jeweiligen Aufsichtsbehörden verabschiedet worden sind.[149] Die Vorschriften hierzu und der Inhalt des Vertrages werden in Art. 28 Abs. 3 DSGVO geregelt. Abs. 3 S. 1 Hs. 2 DS-GVO legt die Inhalte, Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen und die Rechte und Pflichten des Verantwortlichen fest, während S. 2 diese noch einmal konkretisiert. Hier werden beispielsweise die Regelungen zur Weisungsgebundenheit oder zur Löschung bzw. Rückgabe der personenbezogenen Daten nach der Verarbeitung verlangt. Legt ein Auftragsverarbeiter entgegen den Bestimmungen der Verordnung die Zwecke und Mittel der Verarbeitung fest, gilt er gemäß Art. 28 Abs. 10 DS-GVO in Bezug auf diese Verarbeitung als Verantwortlicher. Den Auftragsverarbeiter treffen die Pflichten wie beispielsweise aus Art. 24 DS-GVO oder Art. 25 DS-GVO nicht unmittelbar, da er kein Verantwortlicher i.S.d. Gesetzes ist. Jedoch darf ein Verantwortlicher nur solche Auftragsverarbeiter einsetzen, die diese Pflichten erfüllen und somit sind diese mittelbar betroffen.[150] Die Verantwortung für die Verarbeitung trägt grundsätzlich weiterhin der Verantwortliche, da er wie bereits erwähnt über die Zwecke und Mittel entscheidet. Eine Mitverantwortung wird dem Auftragsverarbeiter aber auch an weiteren Stellen der DS-GVO zugeschrieben, die ausdrücklich an ihn adressiert sind.[151] Beispielsweise ist er verpflichtet,

- gemäß Art. 30 Abs. 2 DS-GVO ein Verzeichnis von Verarbeitungstätigkeiten zu führen,
- nach Art. 31 mit der Aufsichtsbehörde zusammenzuarbeiten,
- die Sicherheit der Verarbeitung (technische und organisatorische Maßnahmen) nach Art. 32 Abs. 1 DS-GVO zu gewährleisten,
- gemäß Art. 33 Abs. 2 DS-GVO Datenschutzverletzungen unverzüglich dem Verantwortlichen zu melden oder
- einen Datenschutzbeauftragten zu bestimmen, wie in Art. 37 Abs. 1 DS-GVO geregelt.

Art. 83 Abs. 4 lit. a) DS-GVO sanktioniert einen Verstoß gegen die Auswahlverantwortung mit einem Bußgeld. Wurde ein geeigneter Auftragsverarbeiter ausgewählt, darf dieser nach Art. 28 Abs. 2 DS-GVO ohne schriftliche Genehmigung des Verantwortlichen keinen weiteren Auftragsverarbeiter hinzuziehen. Die schriftliche Form führt häufig zu Kritik, da die in Abs. 9 ermöglichte elektronische Form dadurch in vielen Fällen leerzulaufen droht.[152] Erfolgt eine gesetzeskonforme Beauftragung eines weiteren Auftragsverarbeiters, müssen nach Art. 28 Abs. 4 DS-GVO sämtliche Datenschutzpflichten, die in dem Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Abs. 3 festgelegt worden sind weitergegeben werden. Die Haftungsregelung des Art. 28 Abs. 4 DS-GVO zeigt, dass der Verantwortliche, der Auftragsverarbeiter und der Unterauftragsverarbeiter in dieser Hinsicht (unter anderem gemäß Erwägungsgrund 13 zur DS-GVO) gleich zu behandeln sind und sie dadurch jeweils eine eigene Motivation einer gesetzeskonformen Verarbeitung durch ihren

[149] Vgl. *Datenschutzkonferenz*: „Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO“, URL: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf, S. 2, Abruf: 21.10.2020.
[150] Vgl. *Martini, Mario,* in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 2. Aufl., C.H. Beck, München 2018, DS-GVO Art. 28 Rn. 19 f.
[151] Vgl. *Wächter, Michael*: Datenschutz im Unternehmen, 5. Auflage, C.H. Beck, München 2017, Rn. 982.
[152] Vgl. *Jaspers, Andreas; Jacquemain, Tobias*: „Datenschutz-Grundverordnung – Praxiserfahrungen und Evaluation Aus der Sicht von Datenschutzbeauftragten“, in: Datenschutz und Datensicherheit 05/2020, S. 298

Vertragspartner entwickeln.[153] Eine Auftragsverarbeitung in einem Drittstaat ist, anders als noch im BDSG a.F., ausdrücklich möglich. Hierfür sprechen die Erwähnungen in Art. 3 Abs. 2 DS-GVO, Art. 46 Abs. 2 lit. e) DS-GVO oder auch Erwägungsgrund 80 zur DS-GVO bezüglich der Benennung eines Vertreters eines Auftragsverarbeiters ohne Niederlassung in der Europäischen Union. Selbstredend müssen dabei die Voraussetzungen der Art. 44 ff. DS-GVO zur Übermittlung personenbezogener Daten an Drittländer vorliegen.[154] Bei einer solchen Übermittlung der personenbezogenen Daten in ein sogenanntes Drittland, muss gemäß den dortigen Regelungen eine Zweistufenprüfung der Zulässigkeit durchgeführt werden. In der ersten Stufe wird zunächst die grundsätzliche Rechtmäßigkeit der Verarbeitung geprüft, welche hier in der Auftragsverarbeitung vorliegend bejaht werden kann. Da diese Anforderung erfüllt ist, müssen somit in der zweiten Stufe die Vorschriften der Art. 44 ff. DS-GVO eingehalten werden. Nach Art. 45 DS-GVO dürfen personenbezogene Daten wie bereits dargestellt an ein Drittland außerhalb der EU/des EWR übermittelt werden, wenn die EU-Kommission dem jeweiligen Land ein angemessenes Datenschutzniveau bescheinigt und es dadurch zu einem sogenannten sicheren Drittland wird. Für den Transfer der Daten in unsichere Drittländer müssen gemäß Art. 46 DS-GVO geeignete Garantien beispielsweise in Form von Standarddatenschutzklauseln vorliegen, die von der Kommission vorgegeben werden. Vor allem im Zuge des sogenannten Schrems II-Urteils EuGH bezüglich der Unwirksamkeit des Privacy Shields kamen Unsicherheiten hinsichtlich eines ausreichenden Niveaus der Standarddatenschutzklauseln auf. Diese Kritik wurde nun aufgegriffen und das Schrems II-Urteil in neuen Entwürfen der Standarddatenschutzklauseln berücksichtigt. In einer Stellungnahme des Europäischen Datenschutzausschusses und des EU-Datenschutzbeauftragten Wojciech Wiewiórowski vom 15. Januar 2021 werden diese Änderungen begrüßt und ein besseres Schutzniveau erhofft.[155] Eine weitere Möglichkeit sind verbindliche interne Datenschutzvorschriften nach Art. 47 DS-GVO, die oft auch im Deutschen als Binding Corporate Rules bekannt sind. Liegen die Voraussetzungen beider Stufen vor, kann eine Auftragsverarbeitung auch in Drittländern erfolgen. Das Haftungsrisiko für Auftragsverarbeiter ist mit der DS-GVO stark angestiegen, was auf die, in Erwägungsgrund 13 zur DS-GVO genannten, grundsätzlichen Gleichbehandlung der Verantwortlichen und Auftragsverarbeiter zurückzuführen ist. Zu unterscheiden ist hierbei zwischen der Haftung gegenüber den Betroffenen und der im Vorgang erläuterten Haftung gegenüber dem Auftraggeber bzw. dem Verantwortlichen. Gegenüber Betroffenen haften beide Parteien gesamtschuldnerisch für materiell und immateriell entstandenen Schaden, wobei der Schadensbegriff gemäß Erwägungsgrund 146 zur DS-GVO weit auszulegen ist.[156] Jedoch haftet ein Auftragsverarbeiter gemäß Art. 82 Abs. 2 DS-GVO nur dann, wenn er seinen speziell auferlegten Pflichten der DS-GVO nicht nachkommt oder wenn er rechtmäßig erteilte Weisungen des Verantwortlichen nicht beachtet oder ihnen zuwiderhandelt. Daneben können aufsichtsbehördliche Untersuchungs- und Abhilfebefugnisse gemäß Art. 58 DS-GVO in Betracht kommen. Bezüglich des Verhängens von Bußgeldern kommt bei der Konstellation der Auftragsverarbeitung insbesondere Art. 83 Abs. 3 und 4 DS-GVO zur Anwendung. Aufgrund der neuen Verordnung stellt sich oft die Frage wie mit Altverträgen umzugehen ist, inwiefern diese umzustellen bzw.

[153] Vgl. *Klug Christoph,* in: Gola, Peter (Hrsg.): Datenschutz-Grundverordnung, 2. Aufl., C.H. Beck, München 2018, Art. 28 Rn. 14.
[154] Vgl. *Tinnefeld, Marie-Theres; Buchner, Benedikt; Petri, Thomas; Hof, Hans-Joachim*: Einführung in das Datenschutzrecht, 7. Aufl., De Gruyter, Oldenbourg 2020, S. 281.
[155] Vgl. *European Data Protection Board*: "EDPB & EDPS adopt joint opinions on new sets of SCCs", URL: https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinions-new-sets-sccs_en, Abruf: 19.01.2021.
[156] Vgl. *Klug Christoph,* in: Gola, Peter (Hrsg.): Datenschutz-Grundverordnung, 2. Aufl., C.H. Beck, München 2018, Art. 28 Rn. 18 ff.

neu zu verhandeln sind und wie sich die Regelungen des BDSG a.F. im Vergleich zur DS-GVO unterscheiden. Weitgehend entsprechen die Anforderungen an die Auftragsverarbeitung des § 11 BDSG a.F. denen des Art. 28 DS-GVO. Die meisten Fragen dürften sich über die Vertragsauslegung lösen lassen[157], jedoch besteht in bestimmten Punkten auch ein Anpassungsbedarf. Die Datenschutz-Folgenabschätzung ist ein neu eingeführtes Instrument der DS-GVO und wurde somit in den Altverträgen nicht beachtet. Hier trifft den Auftragsverarbeiter eine Unterstützungspflicht. Fällt die Verarbeitung unter die Kriterien des Art. 35 Abs. 3 DS-GVO, also eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 DS-GVO oder eine systematische umfangreiche Überwachung öffentlicher Bereiche, ist eine Anpassung also zwingend notwendig. Ebenso werden die Regelungen zur grenzüberschreitenden Auftragsverarbeitung von § 11 BDSG a.F. nicht vollständig entsprechend der DS-GVO abgebildet. Sollte die Verarbeitung nicht ausschließlich in Deutschland erfolgen, müssen die Altverträge dementsprechend aktualisiert werden. Der Regelungsgehalt bezüglich der TOMs des BDSG a. F. und der DS-GVO sind vergleichbar. Vor dem Hintergrund der hohen Bußgelder und der strengeren Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO empfiehlt es sich die TOMs auf die Vorgaben der DS-GVO zu überprüfen und gegebenenfalls anzupassen. Die Anpassungsbedürftigkeit von Altverträgen hängt also vom Einzelfall ab, während die TOMs in jedem Fall auf den DS-GVO-Standard überprüft werden müssen. [158]

Im Rahmen der Auswahlverantwortung muss der Auftragsverarbeiter wie bereits erwähnt, hinreichend Garantien dafür bieten, dass geeignete TOMs so durchführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der Verordnung erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Daraus ergibt sich zunächst eine Verpflichtung zur Überprüfung der TOMs im Vorfeld der Auftragsverarbeitung. Genehmigte Zertifizierungsverfahren gemäß Art. 42 DS-GVO können dabei nach Art. 28 Abs. 5 DS-GVO als geeignete Kriterien für hinreichende Garantien herangezogen werden. Diese Nachweise entbinden den Verantwortlichen allerdings nicht von seiner Prüfungspflicht.[159] Während mit dem BDSG a.F. noch ein checklistenbasierter Ansatz verfolgt wurde, sind die erforderlichen Maßnahmen in Art. 32 Abs. 1 S. 2 lit. a) – c) DS-GVO, wie dargestellt, nur sehr allgemein umschrieben.[160] Im Gegensatz zu der Vorgängerregelung in § 11 BDSG a.F. wird in Art. 28 DS-GVO keine ausdrückliche Pflicht zur fortlaufenden Überprüfung während des Auftragsverarbeitungsverhältnisses auferlegt. Trotzdem kann auch unter der Anwendung der DS-GVO von einer Pflicht zur regelmäßigen Überprüfung der TOMs ausgegangen werden. Da der Verantwortliche nur Auftragsverarbeiter einsetzen darf, die geeignete TOMs bieten, müssen diese konsequenterweise nicht nur vor der Beauftragung, sondern ebenfalls während der Laufzeit überprüft werden um dieser Vorschrift gerecht zu werden.[161] Zum einen ergibt sich das bereits aus der allgemeinen Rechenschaftspflicht des Art. 5 Abs. 2 DS-GVO

[157] Vgl. *Hartung, Jürgen; Büttgen, Lisa*: „Die Auftragsverarbeitung nach der DS-GVO“, in: Datenschutz und Datensicherheit, 09/2017, S. 554.
[158] Vgl. *Gürtler, Paul*: „Praxisfragen der Auftragsverarbeitung“, in: Zeitschrift für Datenschutz, 02/2019, S. 54.
[159] Vgl. *Forgó, Nikolaus; Helfrich, Marcus; Schneider, Jochen,* in: Forgó, Nikolaus; Helfrich, Marcus; Schneider, Jochen (Hrsg.): Betrieblicher Datenschutz. Rechtshandbuch, 3. Aufl., C.H. Beck, München 2019, Teil VII. Kapitel 2. Auftrags(daten)verarbeitung Rn. 73.
[160] Vgl. *Bitkom e. V.*: „Begleitende Hinweise zu der Anlage Auftragsverarbeitung – Leitfaden“, URL: https://www.bitkom.org/sites/default/files/file/import/170515-LF-Auftragsverarbeitung-online.pdf, S. 41, Abruf: 02.11.2020.
[161] Vgl. *Eckhardt, Jens*: DS-GVO: „Anforderungen an die Auftragsverarbeitung als Instrument zur Einbindung Externer“, in: Corporate Compliance Zeitschrift, 03/2017, S. 114.

und der Verantwortung des für die Verarbeitung Verantwortlichen aus Art. 24 DS-GVO.[162] Somit finden die Dokumentations- und Nachweispflichten der DS-GVO selbstredend auch auf den Bereich der Auftragsverarbeitung und der Kontrolle der TOMs Anwendung. Gemäß Art. 5 Abs. 2 DS-GVO muss der Verantwortliche die Einhaltung der Datenschutzgrundsätze nach Art. 5 Abs. 1 DS-GVO nachweisen können. Mit Blick auf das hier behandelte Thema hat der Verantwortliche insbesondere die Kriterien bei der Auswahl eines Auftragsverarbeiters, die Einhaltung der Vorschriften gemäß Art. 32 DS-GVO und die Durchführung und das Prüfungsergebnis der Kontrollen der Auftragsverarbeiter zu dokumentieren.[163] Zum anderen verweist Art. 28 Abs. 3 lit. c) DS-GVO auf Art. 32 DS-GVO und die darin enthaltenen Anforderungen. Dadurch ist gemäß Art. 28 Abs. 3 lit. c) DS-GVO i.V.m. Art. 32 Abs. 1 lit. d) DS-GVO eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs zur Gewährleistung der Verarbeitung durchzuführen. Somit ist eine regelmäßige Kontrolle der TOMs während eines Auftragsverarbeitungsverhältnisses für den Verantwortlichen verpflichtend und erforderlich.[164] Die DS-GVO fordert dabei keine Vor-Ort-Kontrolle, sondern erwähnt vielmehr die Möglichkeit von Zertifikaten oder ähnlichen geeigneten Nachweisen.[165] Eine Vor-Ort-Kontrolle dürfte nach der überwiegenden Auslegung des Gesetzeswortlauts dennoch erfasst sein. Ergänzend unterliegt der Auftragsverarbeiter bestimmten Informationspflichten, die den Nachweis sämtlicher Pflichten der DS-GVO umfasst und eine besondere Treuepflicht mit sich bringen.[166] Bei den Audits hat der Verantwortliche die Möglichkeit der selbstständigen Überprüfung oder der Beauftragung eines Auditors.[167] Aufgrund der Sorgfalts- und Aufsichtspflichten in Unternehmen wie beispielsweise aus §§ 93, 111 Abs. 1 AktG bzw. §§ 43, 52 Abs. 1 GmbHG muss unter Berücksichtigung der Größe des Unternehmens und des Geschäftsmodells in vielen Fällen ein Compliance Management System zur Erfüllung dieser Pflichten etabliert werden. Diese Pflicht unterstreichen zahlreiche Urteile zu diesem Thema, wie das wohl bekannteste Siemens/Neubürger-Urteil.[168] Ein Kernpunkt eines solchen Compliance Management Systems ist die Überprüfungspflicht, wodurch die Wirksamkeit der Organisation und die Einhaltung der gesetzlichen Vorgaben und Unternehmensprozesse laufend überprüft und angepasst werden müssen. Bezüglich solchen Audits lässt der Gesetzgeber z.B. in Art. 24 DS-GVO zwar einen gewissen Spielraum, indem die Unternehmen die Erforderlichkeit ebenfalls anhand der Größe und des Geschäftsmodells des Unternehmens eigenständig beurteilen müssen, jedoch dürfte eine Erforderlichkeit in den überwiegenden Fällen zu bejahen sein. Korrespondierend mit Art. 28 Abs. 3 S. 2 lit. h) DS-GVO muss das Überprüfungsrecht bei der Auftragsverarbeitung vertraglich verankert werden. Da

[162] Vgl. *Hartung, Jürgen,* in: Buchner, Benedikt; Kühling, Jürgen (Hrsg.): Datenschutz-Grundverordnung/BDSG, 2. Aufl., C.H. Beck München 2018, Art. 28 Rn. 60.
[163] Vgl. *Der Bayerische Landesbeauftragte für den Datenschutz*: „Auftragsverarbeitung – Orientierungshilfe“, URL: https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf, S. 21, Abruf 23.09.2020.
[164] Vgl. *Gürtler, Paul*: „Praxisfragen der Auftragsverarbeitung“, in: Zeitschrift für Datenschutz, 02/2019, S. 53.
[165] Vgl. *Bitkom e. V.*: „Begleitende Hinweise zu der Anlage Auftragsverarbeitung – Leitfaden“, URL: https://www.bitkom.org/sites/default/files/file/import/170515-LF-Auftragsverarbeitung-online.pdf, S. 9, Abruf: 02.11.2020.
[166] Vgl. *Voigt, Paul; von dem Bussche, Axel,* in: Voigt, Paul; von dem Bussche, Axel (Hrsg.): Konzerndatenschutz. Rechtshandbuch, 2. Aufl., C.H. Beck, München 2019, S. 212.
[167] Vgl. *Kremer, Sascha*, in: Laue, Philip, Kremer, Sascha (Hrsg.): Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl., Nomos, Baden-Baden 2019, S. 207.
[168] Vgl. *LG München I*, Urteil v. 10.12.2013 - 5HK O 1387/10.

TOMs ein wesentliches Instrument zur Umsetzung dieser Vorschriften und von Compliance-Anforderungen sind, ist dies insbesondere auch hierauf anzuwenden.[169]

3.2.2 Mögliche Vorgehensweisen zur Kontrolle technischer und organisatorischer Maßnahmen

Die Kontrolle der TOMs kann auf verschiedene Weise erfolgen. Geeignete Nachweise können wie erwähnt Zertifizierungen gemäß Art. 40 und 42 DS-GVO sein, darüber hinaus sind Audits eines Unternehmens durch externe Spezialisten eine weitere Möglichkeit der Kontrolle. Ein solches Audit kann in Form von Checklisten und Fragebögen, jedoch auch durch Vor-Ort-Kontrollen erfolgen. In einigen Fällen ist eine Kombination von Fragebögen und Vor-Ort-Kontrollen sinnvoll, wie im weiteren Verlauf der Arbeit dargestellt wird.

3.2.2.1 Zertifizierungen

Die vom Gesetzgeber hoch angedachte Bedeutung von Zertifizierungen lässt sich bereits durch die Aufnahme eines eigenen Artikels in die DS-GVO erahnen. Dabei erfolgt eine Überprüfung des Auftragsverarbeiters durch einen unabhängigen Dritten mit anschließender Zertifizierung. Zu beachten gilt es dabei die Art des Zertifikates, die ausstellende Zertifizierungsstelle, den Geltungsbereich des Zertifikates und die Laufzeit. Dabei gibt es zwei Arten von Zertifikaten, zum einen gibt es Normzertifikate und zum anderen freiwillige Prüfzeichen. Zertifizierungen können beispielsweise von akkreditierten Zertifizierungsstellen, Wirtschaftsprüfungsgesellschaften, Bundesämtern, Prüfverbänden oder Gutachtern erteilt werden. Ein freiwilliges Prüfzeichen stellt lediglich beispielsweise das GS-Zeichen dar. Normzertifikate sind von akkreditierten Zertifizierungsstellen wie Dekra, DeuZert oder dem TÜV ausgestellte Zertifikate. Diese Art von Zertifikaten wird auf Grundlage einer gültigen internationalen Norm wie einer ISO-Norm mit begrenzter Gültigkeit ausgestellt. Während der begrenzten Laufzeit erfolgen zwei Wiederholungsaudits, durch die die fortlaufende Erfüllung der Anforderungen überprüft wird. Nach Ablauf des Zertifikates kann ein Rezertifizierungsaudit durchgeführt und das Zertifikat somit erneut erteilt werden.[170] Eine Zertifizierung kann gemäß Art. 42 Abs. 7 DS-GVO für eine Dauer von maximal drei Jahren erteilt werden und nach Ablauf unter denselben Bedingungen und den einschlägigen Voraussetzungen der Zertifizierung neu zertifiziert werden. Insbesondere bei großen Konzernen ist es wichtig den korrekten Geltungsbereich des Zertifikates zu überprüfen, da eine Zertifizierung auch nur für bestimmte Betriebseinheiten oder Standorte gelten kann.[171] Ein Zertifikat sorgt für ein einheitliches Prüfniveau und soll die Prozesse der Unternehmen vereinfachen. Die individuelle Kontrolle jedes einzelnen Auftragsverarbeiter ist für den Verantwortlichen aufgrund der häufigen praktischen Anwendung mit sehr hohem Personal- und Zeitaufwand verbunden. Auf der anderen Seite sieht sich ein Auftragsverarbeiter vielen, sehr ähnlichen Kontrollen durch sämtliche Verantwortliche ausgesetzt. Auch aus deren Sichtweise werden dadurch enorm viele Ressourcen gebunden. Anhand geeigneter Zertifizierungsverfahren gemäß den Anforderungen der Art. 42 f. DS-GVO kann der Verantwortliche also grundsätzlich von der Umsetzung geeigneter TOMs ausgehen[172] Laut dem Bayerischen Landesamt für Datenschutzaufsicht liegt der Zweck der Zertifizierung unter anderem darin, den Kunden und Geschäftspartnern die Einhaltung da-

[169] Vgl. *Krätschmer, Stefan*, in: Specht, Louisa; Mantz, Reto (Hrsg.): Handbuch Europäisches und deutsches Datenschutzrecht, 1. Aufl., C.H. Beck, München 2019, S. 145 ff.
[170] Vgl. *Koglin, Olaf,* in: Lachenmann, Matthias; Koreng, Ansgar (Hrsg.): Formularhandbuch Datenschutzrecht, 2.Aufl., C.H. Beck, München 2018, E.II.2. Formular zur Prüfung der TOMs Rn. 12.
[171] Vgl. *Koglin, Olaf,* in: Lachenmann, Matthias; Koreng, Ansgar (Hrsg.): Formularhandbuch Datenschutzrecht, 2.Aufl., C.H. Beck, München 2018, E.II.2. Formular zur Prüfung der TOMs Rn. 12.
[172] Vgl. *Schäfer, Christoph; Fox, Dirk*: „Zertifizierte Auftragsdatenverarbeitung - Das Standard-ADV-Modell“, in: Datenschutz und Datensicherheit, 11/2016, S. 745 f.

tenschutzrechtlicher Vorgaben darlegen zu können.[173] Gemäß Art. 42 DS-GVO soll den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen Rechnung getragen werden. Das bedeutet die Zertifizierungen sollen sich nicht nur an größere Unternehmen und Konzerne richten, was sich aber in der Praxis z.B. aufgrund teils trotzdem hoher Kosten und weiterer erforderlicher Maßnahmen zunächst noch erweisen muss.[174] Das Gebiet der Zertifizierung ist deutlich von einem Audit zu unterscheiden. Ein Audit kann eine Zertifizierung zur Folge haben, jedoch ist die Zertifizierung keine logische Folge eines Audits, welches lediglich die Überprüfung an sich darstellt. Die wohl populärste und meistverwendete Zertifizierung in diesem Bereich ist die International Organisation for Standardization (ISO)/International Electrotechnical Commisssion (IEC) 27001. Die weltweit anerkannte Zertifizierung zielt grundsätzlich auf Informationssicherheits-Managementsysteme und die Sicherheit von sämtlichen Informationen, Daten und Systemen ab. In dieses Cluster fallen demnach auch personenbezogene Daten und TOMs zu deren Schutz. Die ISO/IEC 27001 und die datenschutzrechtlichen Bestimmungen der DS-GVO überschneiden sich in einigen Bereichen. Die in Art. 5 DS-GVO geregelten Datenschutzgrundsätze Vertraulichkeit, Verfügbarkeit und Integrität von personenbezogenen Daten sowie die Bestimmungen zu den TOMs aus Art. 32 DS-GVO finden sich in gewisser Weise auch in den Ausführungen der Zertifizierung wieder. Dabei sollen z.B. interne und externe Probleme identifiziert werden, die sich auf Sicherheitsprogramme auswirken können oder für eine Aufrechterhaltung und Dokumentation der Programme sorgen. Des Weiteren erfolgt innerhalb der ISO/IEC 27001 eine Klassifizierung von Daten, wodurch die Einhaltung der datenschutzrechtlichen Vorgaben zusätzlich erleichtert wird. Die DS-GVO beruht auf risikobasierten Ansätzen, die auch im Zuge der Zertifizierung wiederzufinden sind. Speziell auf Art. 28 DS-GVO bezogen werden die Weisungsgebundenheit und die Überwachung und Kontrolle der Auftragsverarbeiter zertifiziert. Die ISO/IEC 27001 deckt dabei keinesfalls alle Anforderungen der DS-GVO ab, jedoch können geeignete TOMs nachgewiesen werden.[175]

3.2.2.2 Fragebogen/Checkliste

Eine weitere Methode der Kontrolle von TOMs bei Auftragsverarbeitern ist das Erstellen und Abarbeiten von Fragebögen bzw. Checklisten mit spezifischen Fragen zur Umsetzung. Bei dieser Vorgehensweise müssen Fragebögen entwickelt und durch den Dienstleiser ausgefüllt werden. Befragungen zu diesen Maßnahmen können auch im Zuge allgemeiner Datenschutzaudits anhand von Ergänzungen des Basisfragebogens durchgeführt werden. Unabhängig davon wird der entsprechende Fragebogen an die jeweiligen Auftragsverarbeiter gesendet und muss ausgefüllt zurückgeschickt werden. Der Auftragsverarbeiter kreuzt die zutreffenden und bei ihm umgesetzten TOMs an bzw. beschreibt diese. Die Checkliste sollte alle relevanten Aspekte wie Zutritts-, Zugangs- und Zugriffkontrollen, Datenweitergabe oder die betriebliche Organisation und deren Abläufe enthalten. Werden darüber hinaus zusätzliche Maßnahmen getroffen, die in dem Fragebogen nicht enthalten sind, kann die Liste ergänzt werden. Im Nachgang wird bewertet inwieweit die Maßnahmen ausreichend und geeignet sind, um den gesetzlichen Anforderungen zu entsprechen. Den einzelnen Maßnah-

[173] Vgl. *Der Bayerische Landesbeauftragte für den Datenschutz*: „Arbeitspapier zur Zertifizierung – Art. 42 DS-GVO“, URL: https://www.lda.bayern.de/media/baylda_ds-gvo_2_certification.pdf, S. 5, Abruf 18.11.2020

[173] Vgl. *Plath, Kai-Uwe,* in: Plath, Kai-Uwe (Hrsg.): DSGVO/BDSG, 3. Aufl., Otto Schmidt, Köln 2018, Art. 28 Rn. 8.

[174] Vgl. *Bertermann, Nikolaus; Piltz, Carlo,* in: Lachenmann, Matthias; Koreng, Ansgar (Hrsg.): Formularhandbuch Datenschutzrecht, 2.Aufl., C.H. Beck, München 2018, C.I. Datenschutzaudit Rn. 1 ff.

[175] Vgl. *TÜV Süd AG*: „ISO/IEC 27001 - ISMS-ZERTIFIZIERUNG“, URL: https://www.tuvsud.com/de-de/dienstleistungen/auditierung-und-zertifizierung/cyber-security-zertifizierung/iso-27001, Abruf: 23.11.2020.

men wird je nach Wichtigkeit und Bedeutung die Eintrittswahrscheinlichkeit eines daraus entstehenden Schadens zugeordnet. Die Erforderlichkeit und Dringlichkeit der Umsetzung der Maßnahmen wird danach in die Kategorien „empfohlen“, „verpflichtend“ und kritisch“ eingeordnet. Aus diesen Kategorien entstehen Fristen für die Umsetzung bzw. die Planung der Umsetzung, deren Einhaltung nachgewiesen werden sollte. Aus der Anzahl der erfolgten bzw. nicht erfolgten Umsetzung der Maßnahmen der einzelnen Kategorien können in einem Prüfbericht Empfehlungen hinsichtlich des weiteren Vorgehens mit dem jeweiligen Dienstleister abgeleitet werden. Dabei wird die gesamte Eintrittswahrscheinlichkeit eines Schadens nach Auswertung der Erfüllung aller TOMs von sehr niedrig bis sehr hoch bewertet. Ein Prüfbericht beinhaltet darüber hinaus Angaben zur Prüfung selbst wie den Inhalt der Prüfung, die Prüfungszeit und den Ort, den Prüfer, Kriterien der Bewertung und eine Handlungsempfehlung. Der Bericht kann schlussendlich als Ergebnis dem jeweiligen Dienstleister übergeben werden. Eine Automatisierung der Prozesse kann bei der Kontrolle anhand solcher Checklisten und Fragebögen mit einer großen Zeitersparnis und Sicherheit des Vorgangs einhergehen. Mit Hilfe von Datenschutzmanagementsoftware, die beispielsweise von Anbietern wie OneTrust oder 2B Advice auf dem Markt zu finden ist, kann die Datenschutzverwaltung optimiert werden. Bezogen auf die Kontrolle der TOMs anhand von Fragebögen oder Checklisten kann eine solche Software den Aufwand und die Kosten aufgrund von Zeit- und Personaleinsparungen senken. Die entsprechenden Fragebögen können automatisch in einem festgelegten Rhythmus an die jeweiligen Auftragsverarbeiter versendet werden. Somit wird die gesetzlich geforderte, turnusmäßige Überprüfung ohne großen Aufwand sichergestellt. In standardisierten Fällen dürfte eine automatische Auswertung der Fragebögen möglich sein, die ein Eingreifen lediglich bei Bestehen von Risiken oder bei offenen Punkten erfordern. Die tatsächlichen Möglichkeiten der Umsetzung dieser Funktionen können nur durch eine individuelle Beratung durch die entsprechenden Anbieter erörtert werden.

3.2.2.3 Vor-Ort-Kontrolle

Die vermutlich aufwändigste Herangehensweise stellt die Vor-Ort-Kontrolle dar. Zunächst muss auch hier eine Checkliste, der zu überprüfenden TOMs erstellt werden. Dafür kann eine Liste, wie unter Kapitel 3.2.2.2 erarbeitet, als Grundlage verwendet werden oder aber stichprobenartig eine Überprüfung bestimmter Aspekte festgelegt werden. Ein Auditteam prüft anhand dieser Festlegungen vor Ort physisch die Umsetzung von Maßnahmen wie die Protokollierung von Besuchern, Alarmanlagen oder die Verschlüsselung von Datenträgern bei dem Dienstleister. Im Anschluss kann auch hier ein Prüfbericht erstellt werden und auf Basis der identischen Risikobewertung wie bei der reinen Prüfung anhand von Fragebögen eine Empfehlung ausgesprochen werden. Durch eine Vor-Ort-Kontrolle durch den Auftragsverarbeiter wird der Aufwand eines Selbstaudits und dadurch möglicherweise nicht vollständig valide Ergebnisse vermieden. Gemäß Art. 28 Abs. 3 lit. h) DS-GVO muss die Auftragsverarbeitungsvereinbarung vorsehen, dass Überprüfungen – einschließlich Inspektionen – die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, vom Auftragsverarbeiter ermöglicht werden und dieser dazu beiträgt. Ansonsten wäre es für den Verantwortlichen unmöglich seinen verbliebenen Pflichten nachzukommen.[176] Die gesetzliche Mitwirkungspflicht und damit die Kontrolle der TOMs, insbesondere Vor-Ort-Kontrollen, dürfen daher auch nicht von einem Entgelt abhängig gemacht werden.

[176] Vgl. *Der Bayerische Landesbeauftragte für den Datenschutz*: „Aktuelle Kurz-Information 6 - Keine gesonderte Entgeltpflicht für Kontrollen bei der Auftragsverarbeitung“, URL: https://www.datenschutz-bayern.de/datenschutzreform2018/aki06.pdf, S. 1, Abruf 13.01.2021.

Eine solche Vereinbarung würde einem ordnungsgemäßen Audit entgegenstehen.[177] Dadurch würde die Kontrolle etwas Außergewöhnliches suggerieren, was dem Verantwortlichen nicht zusteht und eine abschreckende Wirkung entfalten. Der Auftragsverarbeiter kann die ihm entstehenden Kosten lediglich im Voraus in das Angebot der hauptvertraglichen Leistung einpreisen. Dadurch wird eine Vor-Ort-Kontrolle insofern nicht von einem Entgelt abhängig gemacht, als der Verantwortliche die Vertragsbeziehung von Beginn an ablehnen kann und somit zu keiner entgeltlichen Kontrolle verpflichtet wird. Zu beachten ist die Vereinbarung einer Frist der Ankündigung von Vor-Ort-Kontrollen, um der Rücksichtnahme nach Treu und Glauben gerecht zu werden.[178]

3.2.2.4 Kombination Fragebogen/Checkliste – Vor-Ort-Kontrolle

In einigen Fällen ist auch eine Kombination des einfachen Zusendens der erstellten Fragebögen und einer Vor-Ort-Kontrolle sinnvoll. Zunächst wird, wie in Kapitel 3.2.2.2 ein Fragebogen erstellt und versendet. Nach Rückerhalt der Antworten erfolgt eine Auswertung und in Abhängigkeit des Ergebnisses, der Risikobeurteilung und bei unzureichenden Aussagen kann eine zusätzliche Vor-Ort-Kontrolle zur richtigen Einschätzung notwendig sein. Dabei werden ausschließlich TOMs überprüft, bei denen Unstimmigkeiten ersichtlich sind oder auf Nachfrage keine plausiblen Erklärungen zu einzelnen Maßnahmen geliefert werden können. Somit reduziert sich der Aufwand, da nur bestimmte Maßnahmen physisch überprüft werden müssen, während sich die Validität der Ergebnisse gleichzeitig im Vergleich zu der alleinigen Kontrolle mittels Fragebögen erhöht.

Dem Verantwortlichen stehen somit verschiedene Möglichkeiten der Kontrolle der TOMs zur Verfügung. Bei dieser Überprüfung und Beurteilung müssen unabhängig von der Kontrollvariante gemäß den Art. 24 Abs. 1, 32 Abs. 1 DS-GVO der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigt werden.

4 ANALYSE

Um eine optimale Handlungsempfehlung abgeben zu können, müssen die Möglichkeiten zur Erfüllung der jeweiligen gesetzlichen Verpflichtungen analysiert werden. Dabei werden die einzelnen Attribute der verschiedenen Varianten herausgestellt sowie Vor- und Nachteile gegeneinander abgewogen.

4.1 LÖSCHKONZEPT

Um den datenschutzrechtlichen Anforderungen gerecht zu werden ist es, wie unter Kapitel 3.1.1 dargestellt, unverzichtbar, innerhalb der Organisation klare Vorgehensweisen in Form eines Löschkonzepts zu definieren. Verschiedene Herangehensweisen wirken sich unterschiedlich auf die Effizienz und das Risiko der Umsetzung aus. Die in Kapitel 3.1.2 dargestellten Ansätze werden im Folgenden analysiert, um die optimalen Eigenschaften eines

[177] Vgl. *Der Bayerische Landesbeauftragte für den Datenschutz*: „Auftragsverarbeitung Orientierungshilfe“, URL: https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf, S. 21, Abruf: 16.10.2020.
[178] Vgl. *Der Bayerische Landesbeauftragte für den Datenschutz*: „Aktuelle Kurz-Information 6 - Keine gesonderte Entgeltpflicht für Kontrollen bei der Auftragsverarbeitung“, URL: https://www.datenschutz-bayern.de/datenschutzreform2018/aki06.pdf, S. 2, Abruf 13.01.2021.

Löschkonzepts zu erkennen. Nur so kann ein idealer Lösungsansatz für die betriebliche Praxis gebildet werden.

4.1.1 Löschkonzept nach DIN 66398

Die in Kapitel 3.1.2.1 erläuterte DIN 66398 stellte sich als ausführliche und klar formulierte Orientierungshilfe zur Erstellung eines Löschkonzepts heraus. Definierte Anwendungsbereiche, Begriffe und Erklärungen verschaffen den Beteiligten einen Überblick über das Vorgehen. Ein zusätzlicher Vorteil ist das Beschreiben der Kriterien, anhand welcher die Datenkategorien und Löschfristen festgelegt werden und wie Löschklassen entstehen und die Kategorien darin eingeordnet werden. Durch die klare Darstellung der Verantwortlichkeiten und Prozesse wird die Umsetzung und damit das gesetzeskonforme Vorgehen in den Unternehmen erleichtert. Besonders vorteilhaft ist die klare Schrittabfolge des gesamten Prozesses. Somit kann jeder Beteiligte den aktuellen Schritt nachvollziehen und bekommt zusätzlich eine Orientierungshilfe für die Ausführung zur Verfügung gestellt. Die Darstellung der Löschfristen und Startzeitpunkte anhand einer Matrix führt aufgrund ihrer Übersichtlichkeit zu wenig Missverständnissen während des Prozesses. Wie sich durch die Experten aus der Praxis herausgestellt hat, liegt eine Schwierigkeit in der Identifizierung und Löschung der Daten in allen Systemen innerhalb einer Organisation. Hierfür bietet die DIN 66398 einen speziell auf die Umsetzung bezogenen Ansatz. Allerdings unterscheiden sich die Organisation und die Struktur zwischen verschiedenen Unternehmen oft deutlich, wodurch das Vorgehen bei der Identifikation abweichen kann und anhand der Abläufe und Systeme eine individuelle Umsetzung für das jeweilige Unternehmen erfolgen muss. Dies führt trotz der ausdrücklichen Erwähnung und Ausführung dieses Schrittes weiterhin zu Schwierigkeiten in der Praxis. Darüber hinaus werden die Daten erst spät im Prozess identifiziert, wodurch die Bildung von Datenkategorien und Aufbewahrungsfristen zu ungenau sein kann und somit durch weiteren Aufwand ein Nachteil entsteht. Die Norm verfolgt allerdings auch nicht das Ziel eines allgemeingültigen und ausnahmslos anwendbaren Löschkonzepts, sondern soll lediglich die Rahmenbedingungen darstellen.[179] Durch die fehlende Erfassung der Löschung von unberechtigt erhobenen personenbezogenen Daten, von personenbezogenen Daten nach einem berechtigten Löschbegehren des Betroffenen und von personenbezogenen Daten beim Rückbau von Systemen entstehen Lücken in wichtigen Bereichen. Für die komplette Abdeckung und gesetzeskonforme Umsetzung der gesetzlichen Anforderungen werden also keine vollumfassenden, einheitlichen Rahmenbedingungen bereitgestellt und verschiedene Ansätze müssen herangezogen werden. Durch den zweistufigen Ansatz und die Trennung zwischen der Dokumentation und der Umsetzung kann bei einem Vorgehen anhand dieser Norm zwar die Nachweispflicht erfüllt werden, allerdings kann der komplexe Vorgang der Umsetzung und der hier gewählte Ansatz zu Schwierigkeiten führen. Resümierend bietet die Vorgehensweise gemäß der DIN 66398 Anhaltspunkte, die in einem Löschkonzept hilfreich sein können. Hierzu zählen die Definitionen bestimmter Begriffe und die Kriterien zur Festlegung der Datenkategorien und Löschfristen. Die betriebliche Umsetzung der Vorgaben wurde dagegen sehr allgemein gehalten und ist sehr komplex.

4.1.2 Löschkonzept nach Olaf Koglin

In der von Olaf Koglin dargestellten Variante, welche unter Kapitel 3.1.2.2 beschrieben wurde, liegt der Fokus noch mehr auf einem klaren Rechte- und Rollenkonzept und den Verantwortlichkeiten der Mitarbeiter. Dies kann die Durchsetzung der Vorgaben des Löschkonzepts erheblich vereinfachen und eine vollumfängliche Umsetzung fördern. Im Gegensatz zu dem Löschkonzept nach der DIN 66398 erfolgt dabei keine Aufteilung nach Prozessen und An-

[179] Vgl. *Koglin, Olaf,* in: Lachenmann, Matthias; Koreng, Ansgar (Hrsg.): Formularhandbuch Datenschutzrecht, 2.Aufl., C.H. Beck, München 2018, D.IV. Löschkonzepte Rn. 10 ff.

weisungen über Richtlinien oder Betriebshandbücher, sondern eine direkte Zuteilung der Verantwortlichkeiten und Zuweisung der Aufgaben. Dadurch werden die Aufgaben klar und deutlich zugeordnet und die Aufmerksamkeit gesteigert. Da die Zuordnung für Rollen bzw. Positionen erfolgt, wird die Umsetzung auch bei personellen Veränderungen weiterhin sichergestellt. Aufgrund der ständigen Entwicklungen und Veränderungen ist eine solche Vorgehensweise wichtig, um die Gesetzeskonformität in jeder Situation zu gewährleisten. Bei diesem Konzept wird ein risikobasierter Ansatz verfolgt, woraus die Unternehmen einen betriebswirtschaftlichen Vorteil ziehen können. Ein zu risikoreicher Ansatz kann sich jedoch auch nachteilig auf die Erfüllung der datenschutzrechtlichen Anforderungen auswirken und Bußgelder zur Folge haben. Durch die Benennung sogenannter Datenowner und die gemeinsame Festlegung der Risikofreudigkeit mit allen Beteiligten der Geschäftsleitung und des IT- und Datenschutzbereichs wird allerdings genügend Expertise für diese Entscheidung herangezogen. Der risikobasierte Ansatz ist zwar eines der Kernelemente der DS-GVO, jedoch dient er nicht dazu, den Wegfall bestimmter Maßnahmen zu rechtfertigen und dennoch die Datenschutz-Compliance sicherstellen zu können. Die Vorschriften der DS-GVO müssen dabei selbstredend ungeachtet dessen erfüllt werden, sie sollen durch diesen Ansatz schließlich nicht unterlaufen, sondern ergänzt werden.[180] Des Weiteren können durch das Einbeziehen verwandter Themen wie den anderen Betroffenenrechten oder Informationssicherheitskonzepten bereichsübergreifende Synergien entstehen. Die Definitionen und Vorgaben zur Festlegung der Kriterien und Fristen innerhalb eines Löschkonzepts werden hier hingegen lediglich in einem überschaubaren Umfang erläutert. Dadurch ist eine Bestimmung dieser Größen zunächst schwierig. Die Ausführungen des Vorgehens der Identifikation der personenbezogenen Daten innerhalb der Unternehmen wird bei dieser Herangehensweise ebenso vernachlässigt. Dieser Vorgang gilt als eine der größten Herausforderungen in der Praxis und die unzureichenden Anhaltspunkte zu diesem Thema sind somit als enormer Nachteil zu werten. Ferner wird auch hier keine Lösung für die Löschung im Rahmen eines Löschbegehrens betroffener Personen bereitgestellt. Damit kann auch diese Methode keine Abhilfe für dieses Problem schaffen und für solche Fälle keine klare Vorgehensweise definieren. Zudem fehlen detailliertere Empfehlungen zur physischen Löschung personenbezogener Daten wie beispielsweise in Form von Papierdokumenten. In Summe inkludiert dieses Konzept den risikobasierten Ansatz der DS-GVO und ist nah an den Unternehmen und einer betriebswirtschaftlichen Lösung ausgerichtet. Durch das Rechte- und Rollenkonzept und die Orientierung an Rollen und Positionen kann ein stabiler Prozess gewährleistet werden. Auch wenn diese Verfahrensweise wie dargestellt einige Schwächen aufweist, können daraus mehrere hilfreiche Praktiken für ein optimales Löschkonzept abgeleitet werden.

4.1.3 Löschkonzept nach Wilhelm Berning

Die Methode nach Wilhelm Berning wurde technikbasiert entwickelt. Wie ausführlich unter Kapitel 3.1.2.3 verdeutlicht, handelt es sich dabei um eine sehr komplexe Herangehensweise mit dem Nachteil der Notwendigkeit weitreichender IT-Kenntnisse der meisten Beteiligten. Dies wirkt sich negativ auf das Verständnis und die Umsetzung im gesamten Unternehmen aus. Weiterhin wird der Anwendungsbereich dadurch beschränkt, dass der Aufbau der Tabellen und Datensätze aufgrund der komplexen Strukturen von Beginn an in der vorgegebenen Weise umgesetzt werden müssen. Alle bestehenden Datenbestände müssten somit zunächst in einem komplexen Vorgang in die richtige Form übertragen werden, wodurch ein hoher Zeit- und Kostenaufwand entsteht. Eine solche Vorgehensweise ist im Hinblick auf unternehmensintern entwickelte Systeme bzw. bei der Entwicklung solcher Systeme hilfreich. Jedoch werden in nahezu allen Unternehmen eine Vielzahl verschiedener und unter-

[180] Vgl. *Schröder, Markus*: „Der risikobasierte Ansatz in der DS-GVO - Risiko oder Chance für den Datenschutz?“, in: Zeitschrift für Datenschutz, 11/2019, S. 503.

nehmensexterner Systeme verwendet, auf die diese Vorgehensweise nicht anwendbar wäre. Ein zusätzlicher Nachteil ist, dass physische Datenbestände hierbei nicht behandelt werden und eine weitere Verfahrensweise herangezogen werden müsste. Diese Vorgehensweise stellt vielmehr auf die Umsetzung in den IT-Systemen, als auf eine Hilfestellung während des Prozesses ab. Letztendlich leidet die Verständlichkeit der beteiligten Personen und die anwendungsbezogene Umsetzbarkeit darunter. Für die betriebliche Praxis ist diese Verfahrensweise nicht zu empfehlen.

Aus einem ausgereiften Löschkonzept kann ein vielfältiger Nutzen für den Verantwortlichen abgeleitet werden. Prozesse können effizienter gestaltet bzw. neue, klar definierte Prozesse können eingeführt werden. Durch ein dokumentiertes Löschkonzept lassen sich zusätzlich die datenschutzrechtlichen Pflichten zur Löschung nachweisen. Die Umsetzung eines Löschkonzepts wirkt sich auf den gesamten Datenbestand und damit auf gegebenenfalls zwecklose, redundante Daten oder Altbestände aus. Hierdurch können weiterhin Kosten der Datenmigration und des IT-Betriebs eingespart werden.[181] Das Vorliegen eines solchen Konzepts erleichtert allen Beteiligten die Umsetzung der Vorgaben und dient als Orientierungshilfe. Oft ergeben sich für die Verantwortlichen Schwierigkeiten bei der Definition und der Umsetzung eines Löschkonzepts. Die beschriebenen Methoden beinhalten teilweise gute Ansätze. Die DIN 66398 und die Vorgehensweise nach Olaf Koglin sind sich grundsätzlich sehr ähnlich. Jede Variante hat seine Vorteile, die teilweise in einem Löschkonzept zusammengeführt werden können. Beide Möglichkeiten sind auf einen verständlichen und unabhängigen Prozess ausgelegt. Die Arbeitsweise von Wilhelm Berning ist aufgrund der schwierigen Verständlichkeit für die beteiligten Personen und der komplexen Umsetzung für die hier angestrebte Verwendung nicht zielführend. Die Identifizierung der personenbezogenen Daten in sämtlichen Systemen innerhalb der Unternehmen wird auch bei den beiden erstgenannten Vorgehensweisen vernachlässigt. Dieser Prozess unterscheidet sich zwar zwischen den verschiedenen Unternehmen mit tausenden unterschiedlichen Systemen, jedoch muss eine einheitliche Vorgehensweise dargestellt und empfohlen werden, die auf möglichst viele Konstellationen anwendbar ist. Insbesondere, da dies in der betrieblichen Praxis eine der größten Herausforderungen und einen wichtigen Teil des Löschkonzepts darstellt, für den bisher keine Lösung entwickelt wurde. Eine weitere Lücke in den bestehenden Löschkonzepten ergibt sich durch die nicht behandelten Verfahrensweisen im Falle von Löschbegehren betroffener Personen. In den alltäglichen Betriebsabläufen stellt dieser Vorgang die Unternehmen wie sich herausgestellt hat ebenfalls vor Herausforderungen. Für diese Situationen bietet jedoch keines der beschriebenen Löschkonzepte Anhaltspunkte zu möglichen Abläufen. Um eine bestmögliche Handlungsempfehlung aussprechen zu können genügt also keines der vorliegenden Löschkonzepte vollständig. Insbesondere vor dem Hintergrund der expliziten Hervorhebung der genannten Themen im Rahmen der betrieblichen Herausforderungen in der Praxis müssen die Mängel behoben bzw. die bestehenden Methoden ergänzt werden.

4.2 Kontrolle technischer und organisatorischer Maßnahmen

Aus den dargestellten konzeptionellen Grundlagen in Kapitel 3.2 ergibt sich zweifelsfrei eine Verpflichtung zur Kontrolle der TOMs für den Verantwortlichen. Die verschiedenen dargestellten Vorgehensweisen weisen unterschiedliche Vor- und Nachteile und Wirkungs-

[181] Vgl. *Deutsches Institut für Normung e.V. (Hrsg.)*: DIN 66398, Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Beuth Verlag, Berlin 2016, S. 7 f.

zusammenhänge auf. Schwierigkeiten können bei der Durchführung von Audits bei Auftragsverarbeitern beispielsweise durch nicht vollständig oder wahrheitsgetreu ausgefüllte Fragebögen entstehen. Hierfür soll eine bestmögliche Lösung bereitgestellt bzw. empfohlen werden, wofür die Prozesse analysiert und optimal gestaltet werden müssen.

4.2.1 Zertifizierungen

Das Vorliegen einer Zertifizierung i.S.d. Art. 42 f. DS-GVO ist gemäß der Verordnung eine Methode zum Nachweis geeigneter Garantien dafür, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Die Kontrolle erfolgt durch unabhängige Dritte, wodurch valide Ergebnisse erreicht werden können. Ein weiterer Vorteil liegt dabei in der ausdrücklichen gesetzlichen Erwähnung der Geeignetheit entsprechender Zertifikate. Der Aufwand kann zudem für beide Seiten aber insbesondere für den Verantwortlichen als gering eingestuft werden. Für kleine und mittlere Unternehmen kann dies, wie vom Gesetzgeber gewünscht, beispielsweise durch geringere Überprüfungskosten für den Verantwortlichen ebenfalls Vorteile mit sich bringen. Allerdings muss je nach Zertifizierung nach Ablauf von maximal drei Jahren eine erneute Zertifizierung erfolgen, um diese weiterhin aufrechterhalten zu können. Der Nachweis geeigneter TOMs auf Basis einer Zertifizierung bringt also den Nachteil mit sich, dass das Zertifikat regelmäßig verfallen kann. Bei der Prüfung in der Praxis wird das Vorliegen einer Zertifizierung als Indiz für ein gut aufgestelltes Unternehmen herangezogen, jedoch muss eine zusätzliche Prüfung der vorhandenen Maßnahmen mindestens anhand einer Checkliste erfolgen. Zumal die Formulierung des Gesetzgebers mit Blick auf die Auftragsverarbeitung bei genauer Betrachtung sehr zurückhaltend ist. Art. 28 Abs. 5 DS-GVO besagt, solche Zertifikate können lediglich „als Faktor herangezogen werden, um hinreichende Garantien [...] nachzuweisen“. Darüber hinaus wurde noch keine datenschutzspezifische Zertifizierung genehmigt. Der Berufsverband der Datenschutzbeauftragten Deutschlands und die Gesellschaft für Datenschutz und Datensicherheit entwickelten speziell auf die Auftragsverarbeitung bezogen bereits 2013 den Datenschutzstandard „DS-BvD-GDD-01“22. Der Standard wurde in der Zwischenzeit zwar auf die Regelungen der DS-GVO angepasst, allerdings zieht sich das Genehmigungsverfahren in die Länge. Eine eigens für datenschutzrechtliche Belange entwickelte Zertifizierung kann also noch nicht herangezogen werden.[182] Die dadurch notwendige zusätzliche Prüfung anhand der Checkliste bedeutet einen Mehraufwand und zusätzliche Kosten. Jedoch werden dadurch geeignete TOMs auch im Fall des Wegfalls der Zertifizierung sichergestellt und dieser Nachteil der Zertifizierung wird aufgehoben. Eine Zertifizierung ist grundsätzlich also als geeigneter Nachweis i.S.d. Verordnung anzusehen, dennoch wird bezogen auf die Auftragsverarbeitung zusätzlich eine Überprüfung und Bewertung der TOMs durch eine Checkliste durchgeführt und bewertet. Die Aufnahme der Zertifizierung in die DS-GVO ist ein erster Schritt, der zum Erfolg führen kann. Bisher kann eine Zertifizierung in der Praxis jedoch lediglich als zusätzliche Absicherung dienen und es sind weitere Maßnahmen notwendig, durch welche zusätzliche Kosten entstehen.

4.2.2 Fragebogen/Checkliste

Bei der Überprüfung durch einen Fragebogen/eine Checkliste erfolgt eine Bewertung auf Basis der Antworten der Auftragsverarbeiter. Durch eine optimale Gestaltung können mithilfe des Fragebogens alle TOMs abgedeckt werden. Grundsätzlich muss sich dabei auf die getroffenen Aussagen verlassen werden, was aufgrund möglicherweise falscher Angaben durch den Auftragsverarbeiter einen großen Nachteil darstellen kann. Durch das Erfordernis von Begründungen bei Nichterfüllung der Maßnahmen innerhalb des Fragebogens wird die

[182] Vgl. *Richter, Frederick*: „Zertifizierung unter der DS-GVO - Chance eines erleichterten internationalen Datenverkehrs darf nicht verpasst werden“, in: Zeitschrift für Datenschutz, 02/2020, S. 86.

Möglichkeit einer genaueren Einschätzung geschaffen und versucht diesen Nachteil auszugleichen. Mit der beschriebenen Bewertung der Maßnahmen im Zuge der Checkliste und dem Prüfbericht kann eine Handlungsempfehlung abgeleitet und zusätzlich der Dokumentationspflicht Rechnung getragen werden. Der Aufwand bei einer solchen Kontrolle ist gering und kann in Fällen der Integration der Fragebögen zu den TOMs in allgemeine Datenschutzaudits weiter verringert werden. Somit können zusätzlich Kosten eingespart werden. Ein solches Selbstaudit bietet also eine solide Grundlage für gegebenenfalls weitere detailliertere Schritte der Überprüfung. Die Kosten und der Aufwand sind zudem im Verhältnis zu einer ausführlichen Vor-Ort-Kontrolle gering. Die Validität der Ergebnisse kann in manchen Fällen jedoch nicht vollständig gegeben sein.

4.2.3 Vor-Ort-Kontrolle

Der größte Vorteil einer Vor-Ort-Kontrolle ist das Erkennen der tatsächlich vorliegenden Ist-Zustände bei den Auftragsverarbeitern und die dadurch validen Ergebnisse. Die Kontrolle aller notwendigen Maßnahmen stellt allerdings einen sehr hohen personellen Aufwand und ein kostenintensives Vorgehen dar. Die Kontrolle an sich darf indessen wie dargestellt nicht von einem Entgelt abhängig gemacht werden.[183] Gleichzeitig werden die Nachteile eines Selbstaudits und die möglicherweise nicht vollständig validen Ergebnisse durch den Auftragsverarbeiter dadurch weitgehend vermieden. Die ausschließliche Anwendung einer Vor-Ort-Kontrolle ist in den überwiegenden Fällen also betriebswirtschaftlich nicht umsetzbar. Dies bedeutet hohen zusätzlichen Aufwand und somit zusätzliche Kosten. Jedoch kann die Vorgehensweise dadurch valider gestaltet werden. Diese Methode der Kontrolle der TOMs kann dabei helfen aussagekräftige Ergebnisse zu erhalten und Handlungsempfehlungen aussprechen zu können.

4.2.4 Kombination Fragebogen/Checkliste – Vor-Ort-Kontrolle

Die Nachteile der einzelnen Methoden können durch die Kombination eines Fragebogens bzw. einer Checkliste mit einer Vor-Ort-Kontrolle verringert werden. Dabei wird eine Vor-Ort-Kontrolle wie dargestellt lediglich eingesetzt, um Unstimmigkeiten oder kritische Punkte nach Auswertung des Fragebogens zu überprüfen. Damit kann die Richtigkeit der Antworten der Auftragsverarbeiter sichergestellt und eine verlässliche Bewertung und Empfehlung abgegeben werden. Der gezielte Einsatz dieser Kontrollen führt gleichzeitig zu einer Kostenersparnis durch weniger Aufwand.

Die unterschiedlichen dargestellten Möglichkeiten der Kontrolle der TOMs sind allesamt hilfreich, um die Geeignetheit derselben zu erkennen. Jedoch weist jede Kontrollart gewisse Nachteile auf, die durch die Kombination der verschiedenen Varianten ausgeglichen werden können. Die Nachteile eines Selbstaudits anhand von Fragebögen durch den Auftragsverarbeiter können durch eine Vor-Ort-Kontrolle ausgeglichen werden. Durch den vorherigen Einsatz der Fragebögen und die dadurch lediglich gezielte Anwendung der Vor-Ort-Kontrollen können deren Nachteile ebenfalls minimiert werden. Zertifizierungen dienen dabei als zusätzliche Absicherung für alle Beteiligten. Aus den jeweils dargestellten Verfahrensweisen zur Erstellung eines Löschkonzepts und zur Kontrolle der TOMs bei Auftragsverarbeiten und der daraus abgeleiteten Analyse lassen sich nun Handlungsempfehlungen für die betriebliche Praxis aussprechen.

[183] Vgl. *Der Bayerische Landesbeauftragte für den Datenschutz*: „Aktuelle Kurz-Information 6 - Keine gesonderte Entgeltpflicht für Kontrollen bei der Auftragsverarbeitung“, URL: https://www.datenschutz-bayern.de/datenschutzreform2018/aki06.pdf, S. 2, Abruf 13.01.2021.

5 HANDLUNGSEMPFEHLUNGEN FÜR DIE BETRIEBLICHE PRAXIS

Anhand der identifizierten Herausforderungen in der betrieblichen Praxis, den zugehörigen konzeptionellen Grundlagen und der anschließenden Analyse der möglichen Vorgehensweisen können im Folgenden Handlungsempfehlungen für die betriebliche Praxis abgeleitet werden. Dabei sollen bestmögliche Lösungen für die Erstellung und Umsetzung von Löschkonzepten sowie die Kontrolle von TOMs durch den Verantwortlichen bei dessen Auftragsverarbeitern bereitgestellt werden.

5.1 LÖSCHKONZEPT

Wie den vorherigen Kapiteln unschwer entnommen werden kann, ist ein Löschkonzept zur Einhaltung und Umsetzung der einschlägigen datenschutzrechtlichen Anforderungen zwingend erforderlich. Die erläuterten Vorgehensweisen zur Entwicklung eines Löschkonzepts haben jeweils in verschiedenen Bereichen Vor- und Nachteile, stimmen jedoch in manchen Punkten auch überein. Auf Basis dieser Methoden und der Erkenntnisse aus der Literatur und den Experteninterviews soll eine optimale Lösung entwickelt werden. Hierbei soll eine breit anwendbare und bestmögliche Vorgehensweise dargestellt werden. Es wird empfohlen, eine klar strukturierte und praktikable Vorgehensweise in Form eines Löschkonzepts zu definieren, um den erörterten Schwierigkeiten bezüglich eines Löschbegehrens einer betroffenen Person und der systematischen Löschung gemäß Art. 17 DS-GVO entgegenzuwirken.

Zunächst muss der Prozess infolge eines Löschbegehrens, von dem einer systematischen Löschung beispielsweise aufgrund einer Zweckerfüllung unterschieden werden. Zwar bestehen Berührungspunkte innerhalb des Vorgehens, jedoch sollten aufgrund der ansonsten doch deutlich unterschiedlichen Schritte zwei voneinander getrennte Prozesse definiert werden. In der Literatur zu den möglichen Vorgehensweisen bei der Erstellung eines Löschkonzepts werden die Prozesse zum Thema Löschbegehren nur unzureichend beschrieben. Der Blick in die Praxis zeigt, dass die Löschbegehren die Unternehmen über viele verschiedene Kanäle erreichen. Im ersten Schritt ist also das Bewusstsein und die Aufmerksamkeit aller potenziellen Empfänger eines Löschverlangens bezüglich des Erkennens solcher Anfragen und der weiteren Vorgehensweise sicherzustellen. Je nach Organisationsstruktur des Unternehmens, ist anzuraten dies über Richtlinien oder Arbeitsanweisungen und zusätzlich durch Schulung der entsprechenden Mitarbeiter umzusetzen. Die Löschgesuche müssen aufgrund der Antwortfrist unverzüglich an eine einheitliche, für datenschutzrechtliche Themen zuständige Stelle innerhalb des Unternehmens, wie den Datenschutzbeauftragten weitergeleitet werden. Da ein Löschverlangen in der Praxis faktisch oftmals nur z.B. eine Newsletterabmeldung darstellt, bewertet die Datenschutzstelle den Einzelfall und das weitere Vorgehen. Im Falle eines tatsächlichen Löschbegehrens kann gemäß Art. 12 Abs. 6 DS-GVO bei begründetem Zweifel an der Identität des Antragstellers zunächst eine Identitätsprüfung erfolgen. Der Verantwortliche kann zusätzliche Informationen anfordern, die dafür notwendig sind. Dabei genügt ein Abfragen der postalischen Adresse oder des Geburtsdatums, um die Zweifel auszuräumen.[184] Im nächsten Schritt wird die Identifizierung der personenbezogenen Daten des Betroffenen innerhalb des Unternehmens vorgenommen. Dies ist einer der wichtigsten Schritte in diesem Prozess und stellt die Unternehmen in der Praxis

[184] Vgl. *Datenschutzkonferenz*: „Kurzpapier Nr. 6 Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO“, URL: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf, S. 2, Abruf: 15.12.2020.

immer wieder vor große Herausforderungen. In der Literatur ist zu diesem Thema bisher noch wenig umfangreiches Material zu finden. Um einen klaren Überblick zu erhalten und möglichst alle gespeicherten Daten zu erkennen, ist zu empfehlen, die Verantwortlichkeiten nicht nur auf systemübergreifende Bereiche, sondern konkret auf einzelne Systeme aufzuteilen. Somit gibt es einen direkten Verantwortlichen für jedes System und dadurch werden alle Systeme vollständig abgedeckt. Pro Fachbereich ist einer der Systemverantwortlichen zusätzlich für physische Daten des Bereichs zuständig. Je nach Organisation des Unternehmens muss eine Rolle bzw. Position pro Fachbereich oder aus dem Datenschutzbereich bestimmt werden, die an Auftragsverarbeiter übermittelte Daten identifiziert. Diesen Ansatz zur Identifizierung verfolgen in der betrieblichen Praxis viele Unternehmen und große Konzerne. Lokal auf den Rechnern der Mitarbeiter gespeicherte Daten sind schwer auszumachen. Dies kann nur durch das ständige aufmerksam machen aller Mitarbeiter beispielsweise mit Hilfe von grundsätzlichen Datenschutzschulungen oder Schulungen für Neueinsteiger verhindert werden. Auch die Identifizierung muss aufgrund der gesetzlichen Anforderungen möglichst schnell erfolgen. Nach Art. 12 Abs. 4 DS-GVO wird ein Tätigwerden spätestens innerhalb eines Monats gefordert, wodurch die Unverzüglichkeit zwar ohne schuldhaftes Zögern, jedoch in jedem Fall in weniger als einem Monat eintritt. In der Regel dürfte hier ein Tätigwerden innerhalb von zwei Wochen als unverzüglich anzusehen sein.[185] Zur Sicherstellung einer kontinuierlichen Prozessstabilität wird empfohlen die Verantwortlichkeiten auf Rollen bzw. Positionen im Unternehmen zu verteilen. Dadurch können Unsicherheiten und Verzögerungen z.B. bei personellen Veränderungen vermieden werden. Zu diesem Zweck ist ein Dokument mit den jeweiligen Rollen oder Positionen und ihren entsprechenden Rechten zu erstellen. Dieses Dokument ist Bestandteil des Löschkonzepts und muss den zuständigen Stellen ständig in der aktuellen Version zur Verfügung stehen. Im Rahmen des Austritts- bzw. Einstellungsprozesses muss das Dokument je nach Unternehmensorganisation von der rechteverwaltenden Stelle wie beispielsweise dem Access-Management oder dem IT-Bereich herangezogen werden. Dadurch werden die Zugriffsrechte direkt angepasst und sind ständig auf dem neuesten Stand. Darüber hinaus können mit einem solchen Rechte- und Rollenkonzept die allgemeinen Zugriffsrechte und somit weitere wichtige Anforderungen der DS-GVO erfüllt werden. Im Hinblick auf diese Arbeit wird allerdings nur dessen Zusammenhang mit dem Löschkonzept behandelt. Die bereits genannte zuständige Datenschutzstelle im Unternehmen benachrichtigt im Folgenden also beim Vorliegen eines Löschbegehrens unverzüglich alle Systemverantwortlichen, welche schnellstmöglich Auskunft über die, in den jeweiligen Systemen gespeicherten personenbezogenen Daten des Betroffenen geben. Anschließend wird erneut vom Datenschutzbereich geprüft, auf welcher Grundlage die Daten gespeichert werden und welche Aufbewahrungsfristen einer Löschung möglicherweise entgegenstehen. Oftmals können personenbezogene Daten in einigen Systemen gelöscht werden, in anderen werden sie jedoch weiterhin benötigt oder ein Teil der vorhandenen Daten kann in allen Systemen gelöscht werden und nur weniger Angaben werden benötigt. Die Erforderlichkeit einer Löschung wird den entsprechenden Systemverantwortlichen und Auftragsverarbeitern unverzüglich mitgeteilt und muss von diesen gegebenenfalls in Zusammenarbeit mit dem IT-Bereich umgesetzt werden. Aufgrund verschiedener Zwecke der Verarbeitung und Rechtsgrundlagen kann sich die Löschverpflichtung zwischen den Systemen und Datenarten unterscheiden. Derartige Ansätze sind auch in der betrieblichen Praxis wiederzufinden. Für die Umsetzung der Löschung müssen im Vorfeld genaue Vorgaben gemacht werden, um die Probleme und daraus folgenden Unsicherheiten bei diesem Thema in der Praxis vermeiden zu können.

[185] Vgl. *Paal, Boris P.*, in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 2. Aufl., C.H. Beck, München 2018, BDSG Art. 17 Rn. 2.

Physische Daten wie z.B. Papierakten müssen vernichtet bzw. zerstört werden. Bei elektronischen Daten führt eine Zerstörung der Festplatte zwar zum gleichen Ergebnis, jedoch ist dies in der Praxis nicht umsetzbar.[186] Bei der rein physischen Löschung von Dokumenten wird daher empfohlen die Dokumente zu schreddern oder in einem sogenannten Datenschutzbehälter zu entsorgen. Diese Sicherheitsbehälter werden von verschiedenen Dienstleistern bereitgestellt. Die entsprechenden Dokumente werden darin gesammelt und im Anschluss von dem Dienstleister abgeholt und entsorgt. Dabei sollte auf die DIN 66399 Zertifizierung des Auftragnehmers bezüglich des gesamten Vernichtungsprozesses und der Sicherstellung geeigneter TOMs geachtet werden.

Das Vorgehen beim technischen Löschen digitaler Dokumente sollte systemabhängig durchgeführt werden. Wie sich anhand der Erfahrungen der interviewten Datenschutzexperten gezeigt hat, sind die Möglichkeiten je nach System sehr unterschiedlich bzw. teilweise beschränkt. Es wird angeraten, im Voraus für jedes System eine klare Vorgehensweise bzw. eine Definition der Löschung zu konzipieren. Dabei sollten die, in Erwägungsgrund 26 zur DS-GVO genannten objektiven Faktoren zur Feststellung der Identifizierbarkeit natürlicher Personen, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, der zum Zeitpunkt der Verarbeitung verfügbaren Technologie und den technologischen Entwicklungen, berücksichtigt werden. In diesen Prozess sollte neben dem Datenschutzbereich und dem jeweiligen Systemverantwortlichen unbedingt der IT-Bereich eingebunden werden, um alle Möglichkeiten der Systeme erkennen und umsetzen zu können. Einige Systeme erlauben beispielsweise nur ein Überschreiben der Daten. Sollte eine tatsächliche Löschung wie unter Kapitel 3.1 erläutert aufgrund der Systemgegebenheiten nicht möglich sein, muss, wenn möglich zumindest eine ebenfalls in diesem Kapitel dargestellte Anonymisierung z.B. durch Überschreiben der personenbezogenen Daten erfolgen. Sieht ein System keine Möglichkeit der Erfüllung dieser Anforderungen vor, ist anzuraten, dieses außer Betrieb zu nehmen und nicht weiter zu verwenden. Aufgrund der, in der Regel überschaubaren Anzahl solcher Anfragen, ist dieses Vorgehen und die Einzelfallbetrachtung umsetzbar und als pragmatische Lösung zu empfehlen. Der Prozess kann wie folgt dargestellt werden:

[186] Vgl. *Ernst, Stefan,* in: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 2. Aufl., C.H. Beck, München 2018, DS-GVO Art. 4 Rn. 34.

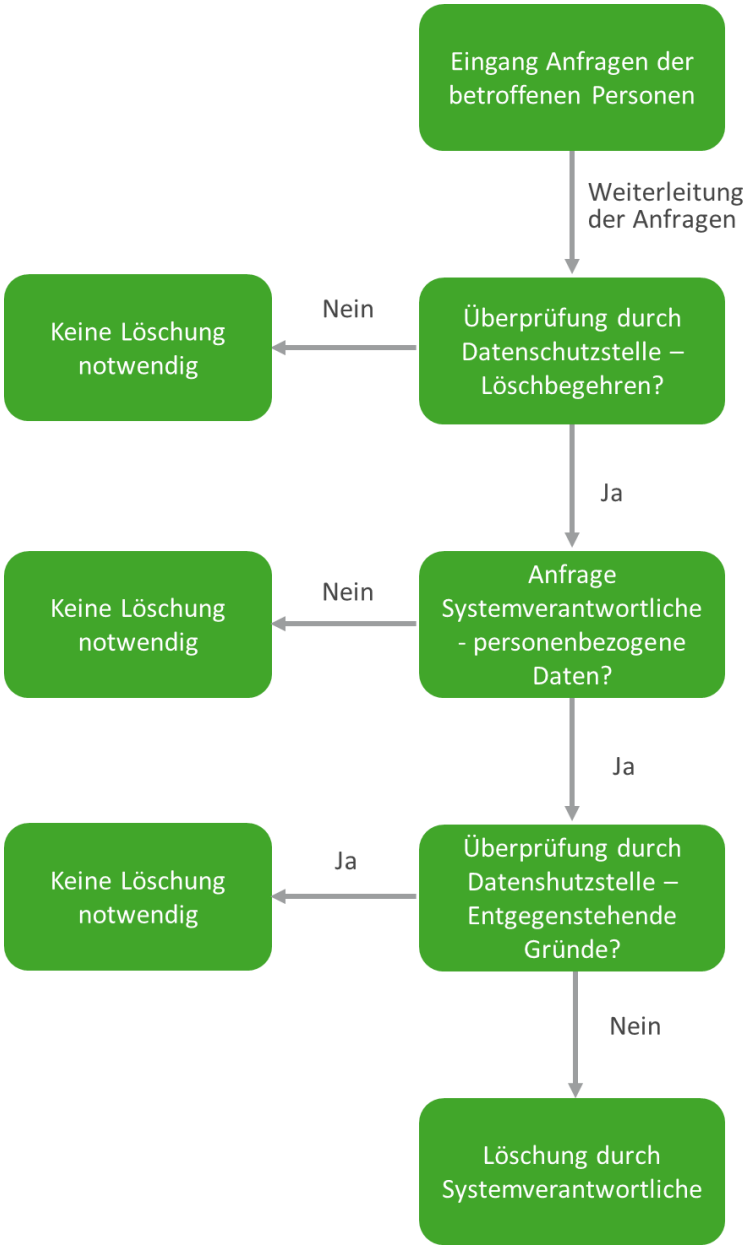

Abb. 2: Löschprozess infolge von Löschbegehren betroffener Personen[187]

Der Prozess zur systematischen Löschung personenbezogener Daten gemäß Art. 17 Abs. 1 DS-GVO wird hier getrennt von dem der Löschung aufgrund eines Löschbegehrens gemäß diesem Artikel entwickelt. Einige Synergien können zwar geschaffen werden, jedoch wird in Anbetracht der doch sehr unterschiedlichen Auslösungsgründe und Einflussfaktoren empfohlen die Prozesse voneinander zu trennen. Um eine systematische Löschung aus den, in Art. 17 Abs. 1 lit. a) – f) DS-GVO genannten Gründen umsetzen zu können, wird folgende Vorgehensweise empfohlen:

1. Datenkategorien bilden

Zur Erfüllung dieser Vorschriften müssen alle personenbezogenen Daten innerhalb eines Unternehmens bezüglich des Eintritts der Löschverpflichtung im Blick behalten werden. Auf-

[187] Eigene Darstellung.

grund der großen Mengen an personenbezogenen Daten wird empfohlen, zunächst Datenkategorien zu erstellen, um die Daten im weiteren Verlauf darunter zusammenfassen zu können. Dadurch wird eine bessere Übersicht geschaffen und das weitere Vorgehen vereinfacht. Die DIN 66398 enthält eine anschauliche Definition des Begriffs. Eine dort sogenannte Datenart wird als „Gruppe von Datenobjekten, die zu einem einheitlichen fachlichen Zweck verarbeitet wird“ bezeichnet.[188] Das bedeutet, personenbezogene Daten mit den gleichen Rechtsvorschriften, was zu denselben oder ähnlichen Aufbewahrungsfristen führt, sollen einer Kategorie zugeordnet werden. Daten mit gleichem Verwendungszweck sind gleichzeitig zu löschen. Die Kriterien zur Einordnung der personenbezogenen Daten in die einzelnen Kategorien müssen klar und deutlich formuliert werden, um im weiteren Verlauf möglichst wenige Fragen der Mitarbeiter aufkommen zu lassen und eine korrekte Zuordnung zu gewährleisten. Beispiele solcher Kategorien können Kundendaten, Mitarbeiterdaten oder Bewerberdaten sein. Je nach Unternehmen können unterschiedliche Kategorien personenbezogener Daten verarbeitet werden, daher müssen diese individuell vom Datenschutzbereich festgelegt werden. Sind bereits Datenkategorien vorhanden werden diese überprüft und gegebenenfalls angepasst. Die Datenkategorien und die dazugehörigen Zuordnungskriterien sollten in Form von Golden Rules als Handbuch für die zuständigen Mitarbeiter aufbereitet werden, um Unsicherheiten zu vermeiden. Zusätzlich sollten die Vorgaben zur Sicherstellung der Umsetzung in Unternehmensrichtlinien und Arbeitsanweisungen übernommen werden.

2. Fristen bestimmen

Im Anschluss an die Definition der Datenkategorien müssen Lösch- bzw. Aufbewahrungsfristen für jede Kategorie bestimmt werden. Für eine praktikable Umsetzung der Fristenfestlegung wird ein Ansatz empfohlen, der sich an der DIN 66398 orientiert. Für jede Datenkategorie muss zunächst geklärt werden, wie lange diese für die Geschäftsprozesse benötigt wird. Dies ist abhängig von den Zwecken der Verarbeitung und der dadurch bestehenden Rechtsgrundlage sowie den darüberhinausgehenden Aufbewahrungsfristen. Nach Ablauf der Frist werden die personenbezogenen Daten im Unternehmen nicht mehr benötigt. Diese sogenannte Vorhaltefrist kann aufgrund der Dauer und der Abläufe innerhalb der Löschprozesse in Unternehmen um eine datenschutzrechtlich vertretbare Frist verlängert werden. Diese Frist wird Regellöschfrist genannt und stellt die späteste Löschung der Daten dar. In der Zeit zwischen der Vorhaltefrist und der Regellöschfrist müssen geeignete TOMs umgesetzt werden, um den Zugriff auf die Daten so weit möglich zu beschränken. In einigen Fällen ist die Verlängerung der Frist datenschutzrechtlich nicht vertretbar und daher nicht möglich und die Vorhaltefrist ist anzuwenden. Es wird empfohlen die Fristen von dem Datenschutzbereich und aufgrund der Abhängigkeit von der Risikostrategie des Unternehmens in Abstimmung mit der Geschäftsleitung zu definieren. Um den Aufwand für den Datenschutzbereich zu minimieren und trotzdem die Hoheit über die Fristen zu behalten und den beteiligten Mitarbeitern eine einfachere Zuordnung der Fristen zu den Daten zu ermöglichen, werden Beispiele in Form einer Matrix zu Verfügung gestellt. Dafür werden sogenannte Löschklassen aus einer Kombination der Vorhaltefrist und bestimmten Startzeitpunkten anhand ausgewählter Datenkategorien definiert. Diese Löschklassen stehen stellvertretend für die Gesamtheit und es sollte möglich sein, alle Kategorien personenbezogener Daten unter einer der Löschklassen einordnen zu können. Somit werden alle Datenkategorien zusammengefasst, die dieselbe Löschfrist und denselben Startzeitpunkt besitzen. Durch die vorgege-

[188] Vgl. *Deutsches Institut für Normung e.V. (Hrsg.)*: DIN 66398, Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Beuth Verlag, Berlin 2016, S. 10.

benen Löschklassen wie beispielsweise Buchhaltungsdaten können die Mitarbeiter ihre jeweils darunterfallenden Datenkategorien ohne weiteres Nachfragen zuordnen. Bei der Zuordnung muss die Standardlöschfrist der Vorhaltefrist entsprechen oder darf nur unwesentlich größer ist. Eine mögliche Differenz muss datenschutzrechtlich in Form der Regellöschfrist vertretbar sein. Ist dies nicht möglich, muss eine andere Löschklasse gewählt werden. Häufig ist bei näherer Betrachtung eine kürzere Vorhaltefrist möglich, anderenfalls kann durch weiteres Unterteilen der Datenkategorie eine passende Einordnung erreicht werden. In Sonderfällen wie z.B. bei Rechtsstreitigkeiten können die Löschfristen von den Standardlöschfristen abweichen. In solchen Fällen können die betroffenen Daten in Absprache mit dem Datenschutzbereich einer anderen Datenkategorie mit einer längeren Löschfrist zugeordnet oder entsprechend gekennzeichnet werden. Anhand der Einordnung in die definierten Standardlöschfristen wird daraus die Regellöschfrist, die für das weitere Vorgehen verwendet wird. Je nach Datenkategorie und ausgewählter Löschklasse kann die zugeordnete Standardlöschfrist der Vorhaltefrist aber auch maximal der Regellöschfrist entsprechen. Dies stellt also die längste mögliche Löschfrist für diese Daten dar. Aus den verschiedenen Datenkategorien lassen sich unterschiedliche Startzeitpunkte der Fristen ableiten. Bei Kundendaten beginnt die Frist beispielsweise ab dem Ende der Beziehung zu laufen oder bei Buchhaltungsdaten ab dem Ende des damit zusammenhängenden Vorgangs. Es ist anzuraten, für die beteiligten Mitarbeiter in einem Dokument, in dem die Regellöschfristen festgehalten sind, die Startzeitpunkte auf die verschiedenen Datenkategorien zu transferieren und beispielsweise in „Ende der Vertragslaufzeit“ anstatt „Ende der Beziehung“ zu übersetzen. Um die Komplexität zu reduzieren und die Verständlichkeit bei den beteiligten Mitarbeitern zu erhöhen sollten die Fristen und Startzeitpunkte auf so viele wie nötig, jedoch so wenige wie möglich begrenzt werden. Die Fristen und Startzeitpunkte müssen dabei ebenfalls derart konkret formuliert werden, dass jeder beteiligte Mitarbeiter versteht, wann die Daten welcher Datenkategorie gelöscht werden müssen. Am Ende dieses Schrittes muss jeder Datenkategorie eine Löschfrist und ein Startzeitpunkt dieser Frist zugeordnet worden sein. Eine Matrix mit den Achsen Startzeitpunkt und Löschfrist hilft dabei, den Mitarbeitern eine verständliche Übersicht an die Hand zu geben. Als Hilfsmittel sollte den Mitarbeitern ein Dokument „Regellöschfristen“ zur Verfügung gestellt werden, welches die Regellöschfristen und Startzeitpunkte der Datenkategorien beinhaltet und klar und verständlich formuliert wurde. Die Einhaltung der gesetzten Löschfristen sollte ebenfalls durch eine Aufnahme des Dokuments in die Unternehmensrichtlinien und Arbeitsanweisungen der zuständigen Mitarbeiter sichergestellt werden.

Identifizieren und zuordnen

Bei der Implementierung dieses Löschkonzepts müssen alle personenbezogenen Daten identifiziert werden. Wird die Identifizierung nicht korrekt durchgeführt oder entstehen dabei Lücken, kann dies zu rechtswidrig gespeicherten personenbezogenen Daten und damit zu Bußgeldern führen. Dabei wird dasselbe Vorgehen empfohlen, wie im Zuge der Löschung aufgrund von Löschbegehren bereits erläutert. Die Systemverantwortlichen ermitteln den Bestand an Daten und sind jeweils für ein System bzw. für physische Daten oder Daten bei Auftragnehmern zuständig. Zunächst müssen die vorliegenden personenbezogenen Daten durch die Systemverantwortlichen, wie unter Schritt 2 dargestellt, anhand der zur Verfügung gestellten Kriterien den entsprechenden Löschklassen der Matrix zugeordnet werden. Nach der erfolgten Zuordnung können die Regellöschfristen aus den Standardlöschfristen der Matrix abgeleitet werden. In Abhängigkeit von der IT-Infrastruktur und in Abstimmung mit dem IT-Bereich muss rechtzeitig eine automatische Meldung beispielsweise über einen Trigger bzw. eine automatische E-Mail-Benachrichtigung über das Eintreten der Löschpflicht eingerichtet werden. Die personenbezogenen Daten müssen dann zum Ablauf der entsprechen-

den Frist gelöscht werden. Eine Löschung muss auch hier, wie zu Beginn dieses Abschnitts im Zuge der Löschung hinsichtlich der Löschbegehren ausführlich beschrieben, anhand klar definierter Anforderungen und Vorgehensweisen und gemäß den gesetzlichen Anforderungen erfolgen. Durch die Trennung der einzelnen Systeme wird sichergestellt, dass personenbezogene Daten gleicher Kategorien, die zu verschiedenen Zwecken in unterschiedlichen Systemen verarbeitet werden, nur in den Systemen gelöscht werden, für die die Rechtsgrundlage entfallen und die Löschfrist eingetreten ist. Dadurch wird auch dem Datenschutzgrundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c) DS-GVO Rechnung getragen, wenn die Verarbeitung der Daten lediglich noch in einem System erforderlich ist und in den anderen Systemen und den physischen Datenbeständen gelöscht werden können.

Pflege des Löschkonzepts:

Die Dokumentation ist ein wichtiger Aspekt, um, wie bereits erläutert, der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO gerecht zu werden und einen Nachweis über das Vorgehen und die Prozesse darlegen zu können. Auch aufgrund des Gestaltungsspielraums der Verantwortlichen hinsichtlich des genauen Vorgehens innerhalb der Löschkonzepts und damit einhergehend zur besseren Nachvollziehbarkeit der getroffenen Entscheidungen ist hierauf wertzulegen.[189] Das Löschkonzept und die damit verbundenen Dokumente, z.B. zur Bestimmung der Datenkategorien oder Löschfristen dienen ebendieser Dokumentation und müssen fortlaufend aktuell gehalten werden. Es wird empfohlen die Verantwortlichkeit dem Datenschutzbereich zuzuschreiben. Bei Änderungen diesbezüglicher Dokumente ist eine zwingende Freigabe durch den Datenschutzbereich erforderlich. Nur so kann ein einheitliches und rechtlich korrektes Vorgehen gewährleistet werden. Während des kompletten Prozesses muss ebenfalls die Aktualität des Rechte- und Rollenkonzepts und damit die korrekten Zugriffsberechtigungen und Verantwortlichkeiten der beteiligten Personen sichergestellt und bei Personaländerungen die Berechtigungen entzogen und unmittelbar neu gewährt werden. Durch die Aufteilung der Zuständigkeiten anhand von Rollen und Positionen kann dies bei Veränderungen direkt und ohne Neubestimmung erfolgen. Es wird angeraten, dies ebenfalls vom Datenschutzbereich in Abstimmung mit dem IT-Bereich und dem Access-Management zu überprüfen.

Durch dieses Löschkonzept wird demnach den Nachweis- und Dokumentationspflichten Rechnung getragen. Das Löschkonzept definiert die notwendigen Prozesse und die darin enthaltenen Dokumente stellen alle diesbezüglichen Informationen zur Verfügung und können die Aufsichtsbehörden, wie gefordert im Falle einer Überprüfung unterstützen. Der Prozess kann demnach folgendermaßen abgebildet werden:

[189] Vgl. *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*: „Hinweise zur Dokumentation einer ordnungsgemäßen Verarbeitung personenbezogener Daten“, URL: https://www.datenschutzzentrum.de/uploads/dokumentation/Hinweise_zur_Dokumentation.pdf, S. 1 Abruf: 11.01.2021.

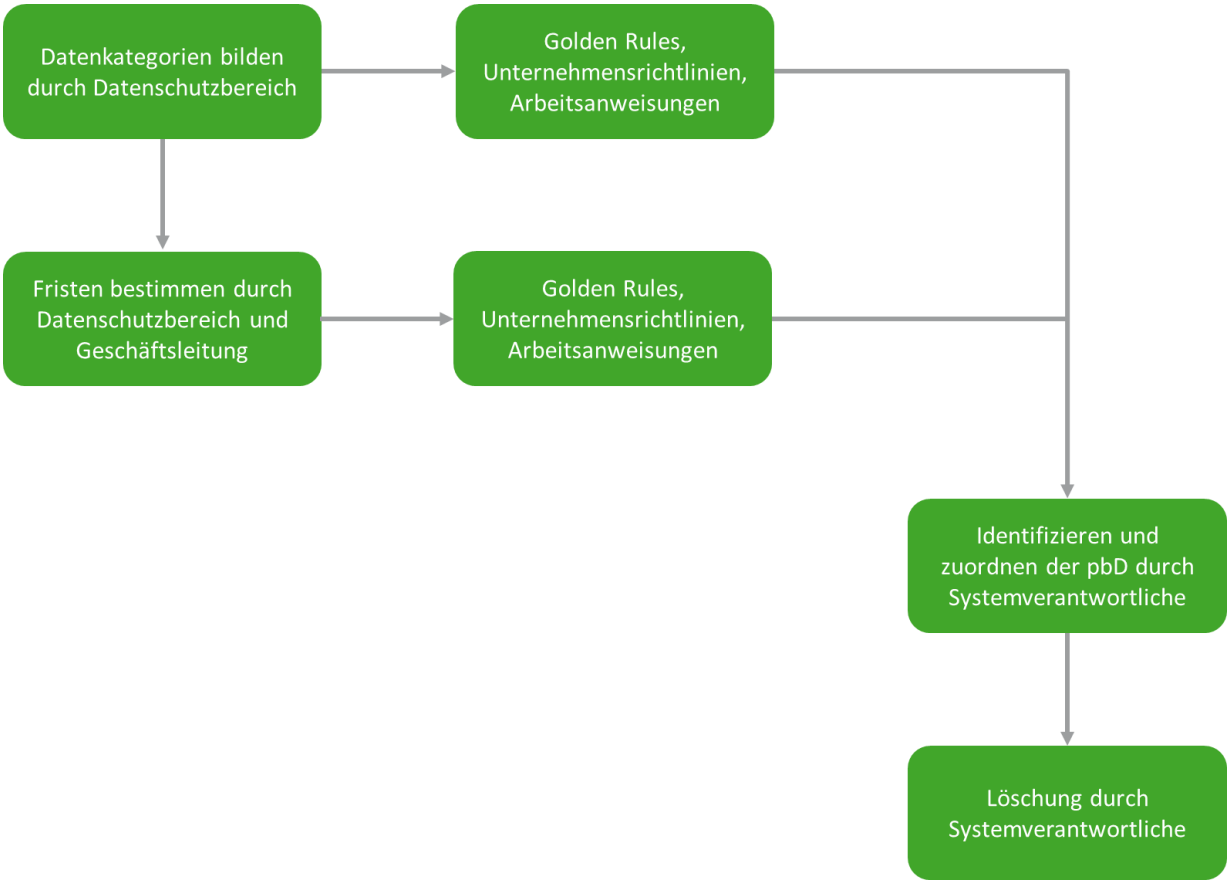

Abb. 3: Löschprozess zur systematischen Löschung[190]

5.2 Kontrolle technischer und organisatorischer Maßnahmen

Wie dem Kapitel 3.2 entnommen werden kann, unterliegt der datenschutzrechtlich Verantwortliche, sowohl einer Auswahlverantwortung gegenüber den Auftragsverarbeitern vor dem Eingehen einer Geschäftsbeziehung als auch einer Verpflichtung zur turnusmäßigen Überprüfung der TOMs während der Laufzeit. Obwohl die Vorgaben bezüglich der TOMs sich von BDSG a. F. zur DS-GVO nicht wesentlich unterscheiden, wird auch im Rahmen von Altverträgen eine solche Überprüfung der jeweiligen Maßnahmen auf den DS-GVO-Standard empfohlen. Somit werden die gestiegenen Anforderungen an die Rechenschaftspflicht erfüllt. Dies kann über die verschiedenen oben dargestellten Vorgehensweisen erfolgen. Im weiteren Verlauf soll die praktikabelste und zweckmäßigste Methode herausgestellt werden.

Das Vorgehen muss möglichst auf alle unterschiedlichen Unternehmen angepasst werden können, um bei jedem neuen Auftrag auf eine einheitliche Methodik zurückgreifen zu können und eine effiziente Arbeitsweise sicherzustellen. Aufgrund des hohen Aufwands einer solchen Überprüfung wird ein praxisorientierter, aber dennoch sicherer Ansatz empfohlen. Dies kann durch eine Kombination einer Selbstauskunft durch den Auftragsverarbeiter und einer Vor-Ort-Kontrolle bei widersprüchlichen Aussagen oder mangelhaften Beschreibungen erfolgen. Im ersten Schritt sollte ein Fragebogen entwickelt werden, in dem sämtliche TOMs in allen Unternehmensbereichen abgefragt werden. Der Umfang und Inhalt eines solchen Fragebogens bzw. einer solchen Checkliste ist abhängig von Faktoren wie der Größe und Or-

[190] Eigene Darstellung.

ganisation des Unternehmens, der Art der verarbeiteten Daten und speziellen Gegebenheiten wie beispielsweise die Ausführung von Tätigkeiten im Homeoffice. Für Auftragsverarbeiter mit lediglich einem kleinen Bürogebäude ergeben sich andere Erforderlichkeiten bezüglich der TOMs als bei großen Konzernen mit großem Betriebsgelände. Ebenso muss bei der Verarbeitung besonderer Kategorien personenbezogener Daten eine ausführlichere Prüfung durchgeführt werden. Ein solcher Fragebogen sollte alle wichtigen Bereiche wie Zutritts-, Zugangs- und Zugriffkontrollen, Datenweitergabe oder die betriebliche Organisation und deren Abläufe abdecken. Je nach Situation muss auch zwischen einem ausführlichen Fragebogen mit vielen speziellen Fragen zu jedem Thema und einem komprimierten Fragebogen mit offen gestellten Fragen abgewogen werden. Bei offen gestellten Fragen müssen die jeweils getroffenen TOMs selbstständig aufgeführt werden. Bei beiden Varianten kann auch das mögliche Vorliegen von Zertifikaten gemäß Art. 42 DS-GVO abgefragt werden. Solche Zertifikate dienen demnach zwar als Nachweis dafür, dass die Vorschriften der Verordnung eingehalten werden, jedoch entbinden sie den Verantwortlichen nicht von dessen Verantwortung und der damit verbundenen Haftung. Der Verantwortliche wird dadurch also nicht von seiner Prüfungspflicht entbunden.[191] Zusätzlich kann eine Zertifizierung aufgrund der in Kapitel 4.2.1 genannten zurückhaltenden Formulierung und der fehlenden spezifischen Datenschutzzertifizierungen nicht als alleinstehende Kontrolle der TOMs dienen. Daher wird der dargestellte Prozess auch bei vorhandener Zertifizierung des Auftragsverarbeiters vollständig durchgeführt. Ein Zertifikat dient bei der Überprüfung allerdings als zusätzliches Indiz für geeignete TOMs bei Unstimmigkeiten und Zweifeln. Um ein valides Ergebnis zu erhalten, müssen einzelne Maßnahmen näher erläutert werden. Für eine optimale Bewertung der Wichtigkeit und Dringlichkeit der jeweiligen TOMs, sollten die einzelnen geprüften Maßnahmen verschiedenen Risikokategorien zugeordnet werden. Die Unterteilung sollte in die Kategorien „empfohlen“, „verpflichtend“ und „kritisch“ erfolgen. Mithilfe dieser Einordnung kann eine Empfehlung bezüglich des weiteren Vorgehens zu der entsprechenden Maßnahme oder mit diesem Auftragsverarbeiter im Allgemeinen ausgesprochen werden. Anhand der Anzahl nicht erfüllter Maßnahmen pro Kategorie kann ebenfalls das Risiko eines Schadenseintritts bewertet werden. Die Rückläufer der Auftragsverarbeiter werden begutachtet und beurteilt. Durch den Zusammenhang verschiedener Fragen zum identischen Bereich und durch diese Erläuterungen können Unstimmigkeiten leichter erkannt werden. In einem solchen Fall kann zunächst erneut Kontakt zu dem Auftragsverarbeiter aufgenommen und versucht werden, ein detaillierteres Bild über die angezweifelten Maßnahmen zu erhalten. Können die Ungereimtheiten dadurch nicht ausgeräumt werden, muss im nächsten Schritt eine Vor-Ort-Kontrolle durchgeführt werden. Durch den vorangestellten Fragebogen müssen hier nur noch die umstrittenen Maßnahmen überprüft werden. Gemäß Art. 28 Abs. 3 lit. h) DS-GVO ist der Auftragsverarbeiter dazu verpflichtet, die für den Nachweis erforderlichen Informationen zur Verfügung zu stellen sowie eine Inspektion auch durch einen vom Verantwortlichen beauftragten Prüfer zu ermöglichen. Bei der gesamten Kontrolle und Bewertung der TOMs müssen gemäß den Art. 24 Abs. 1, 32 Abs. 1 DS-GVO der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigt werden. Mit diesem zweistufigen Vorgehen wird eine hohe Validität der Überprüfung sichergestellt. Da nicht jeder Auftragsverarbeiter vor Ort kontrolliert werden muss und bei den wenigen Vor-Ort-Kontrollen lediglich einzelne Maßnahmen überprüft werden müssen, kann der Aufwand geringgehalten werden. Somit können die fehlenden Kapazitäten und die beschränkte Validität,

[191] Vgl. *Forgó, Nikolaus; Helfrich, Marcus; Schneider, Jochen,* in: Forgó, Nikolaus; Helfrich, Marcus; Schneider, Jochen (Hrsg.): Betrieblicher Datenschutz. Rechtshandbuch, 3. Aufl., C.H. Beck, München 2019, Teil VII. Kapitel 2. Auftrags(daten)verarbeitung Rn. 73.

als die beiden größten Herausforderungen in der Praxis, in diesem Bereich gemeistert werden. Die abschließende Empfehlung soll in Form eines umfänglichen Prüfberichtes abgegeben werden. Ein solcher Prüfbericht sollte zunächst Angaben zum Prüfauftrag und damit zu dem Prüfungsgegenstand, den Prüfern, dem Prüfungszeitraum, -ort und der -art beinhalten. Um eine Transparenz und das Verständnis bei den Akteuren zu erhalten, müssen die Bewertungskriterien ersichtlich gemacht werden. Dadurch kann das nachfolgend dargestellte Ergebnis der Prüfung besser nachvollzogen werden. Dabei müssen die umgesetzten bzw. nicht umgesetzten Maßnahmen der jeweiligen Risikokategorien aufgezeigt werden. Wie zu Beginn dieses Absatzes bereits erläutert kann in Abhängigkeit dieser Kategorisierung das weitere Vorgehen bezüglich der einzelnen Maßnahmen bzw. der Fortführung der Zusammenarbeit empfohlen werden. Bei Nichterfüllung von „empfohlenen“ Maßnahmen wird angeraten, den Auftragsverarbeiter auf diese Empfehlung aufmerksam zu machen. Bei „verpflichtenden“ Maßnahmen sollte die Umsetzung schnellstmöglich in den Planungen des Dienstleisters berücksichtigt werden. Bei einer Nichterfüllung der als „kritisch“ eingestuften Maßnahmen wird empfohlen, die Umsetzung diesbezüglich schnellstmöglich nachweisen zu lassen. Daraus abgeleitet kann abschließend eine Empfehlung zur Unterschrift oder Fortführung eines Vertrages, zur Unterschrift oder Fortführung eines Vertrages unter dem Vorbehalt der Behebung der Mängel gegeben oder von einer Zusammenarbeit abgeraten werden.

Um die Dokumentations- und Nachweispflichten der DS-GVO hierbei zu erfüllen, muss der Verantwortliche, wie unter Kapitel 3.2.1 beschrieben, gemäß Art. 5 Abs. 2 DS-GVO die Einhaltung der Datenschutzgrundsätze nach Art. 5 Abs. 1 DS-GVO nachweisen können. Hier bezieht sich dies auf die Dokumentation der Kriterien bei der Auswahl eines Auftragsverarbeiters, der Einhaltung der Vorschriften gemäß Art. 32 DS-GVO und der Durchführung und des Prüfungsergebnisses der Kontrollen der Auftragsverarbeiter.[192] Hierfür ist der ausgefüllte Fragebogen und der ausführliche Prüfbericht mit sämtlichen beschriebenen Inhalten wie dem Prüfobjekt, dem Inhalt der Prüfung, dem Ergebnis, etc. sehr hilfreich. Diese Dokumente enthalten sämtliche Informationen, die für diesen Teilbereich der Auftragsverarbeitung dokumentiert und nachgewiesen werden müssen. Auch der Auftragsverarbeiter hat bestimmte Dokumentationspflichten, wie die allgemeine Beschreibung der TOMs gemäß Art. 32 Abs. 1 DS-GVO und er muss dem Verantwortlichen alle erforderlichen Informationen zur Einhaltung der Anforderungen gemäß Art. 28 DS-GVO zur Verfügung stellen.[193] Dies kann die Kontrolle der TOMs für den Auditor erleichtern. Der Ablauf kann folgenderweise dargestellt werden:

[192] Vgl. *Der Bayerische Landesbeauftragte für den Datenschutz*: „Auftragsverarbeitung – Orientierungshilfe“, URL: https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf, S. 21, Abruf 23.09.2020.
[193] Vgl. *Der Bayerische Landesbeauftragte für den Datenschutz*: „Auftragsverarbeitung – Orientierungshilfe“, URL: https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf, S. 22, Abruf 23.09.2020.

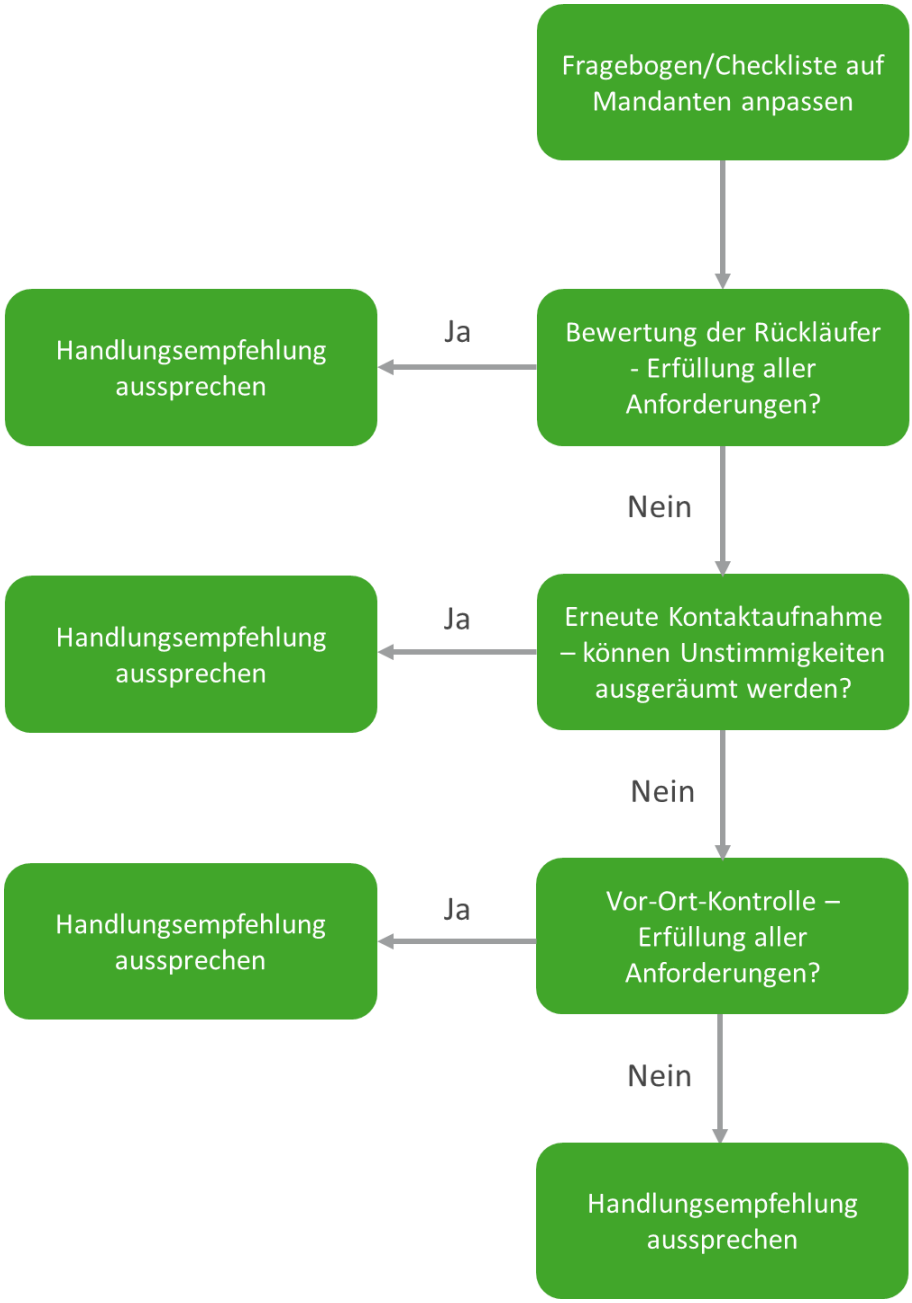

Abb.4: Prozess bei der Kontrolle technischer und organisatorischer Maßnahmen[194]

6 SCHLUSSBETRACHTUNG

Ziel dieser Studie war es, die durch datenschutzrechtliche Anforderungen hervorgerufenen betrieblichen Herausforderungen bezüglich der Datenlöschung und Auftragsverarbeitung zu untersuchen und Handlungsempfehlungen für die betriebliche Praxis zu entwickeln. Dadurch sollen praxisorientierte und verständliche Lösungen und Konzepte für ein gesetzeskonformes Agieren formuliert werden. Dafür wurden zunächst Interviews mit Datenschutzexperten aus verschiedenen Bereichen geführt, um die tatsächlichen alltäglichen Probleme und Herausforderungen in der Praxis ergründen zu können.

[194] Eigene Darstellung.

Bei dieser Untersuchung lies sich herausstellen, dass seit Inkrafttreten der DS-GVO die Aufmerksamkeit für diese Themen und dadurch im Rahmen des Rechts auf Löschung auch die Anzahl an Löschbegehren betroffener Personen gestiegen sind. Hierbei konnten hauptsächlich das Erkennen eines Löschbegehrens aufgrund der verschiedenen Empfangskanäle und das Identifizieren der entsprechenden personenbezogenen Daten als Schwierigkeiten ausgemacht werden. Das Identifizieren stellte sich auch bei einer systematischen Löschung aufgrund, der in Art. 17 Abs. 1 lit. a) – f) DS-GVO genannten Gründe neben der Zuordnung der Löschfristen als eine der größten Herausforderungen heraus. Hierfür fehlen oftmals klare Prozesse und ein einheitliches Vorgehen, um den beteiligten Personen die Umsetzung zu erleichtern.

Als weiterer Themenbereich wurde daneben die Auftragsverarbeitung betrachtet. Dabei konnte eine häufige Anwendung in der Praxis erkannt werden. Durch diese Vielzahl an Auftragsverarbeitern entsteht für den Verantwortlichen bei der regelmäßigen Überprüfung der TOMs ein großer Aufwand. Dabei stellte sich für viele Unternehmen aus personellen und wirtschaftlichen Gründen faktisch eine Unmöglichkeit bezüglich der Durchführung der Kontrolle aller Dienstleister heraus. Wie sich gezeigt hat, wird u.a. aus diesen Gründen vielfach auf eine reine Überprüfung anhand eines Fragebogens bzw. einer Checkliste in Form eines Self-Assessments zurückgegriffen. Dabei muss sich der Verantwortliche auf die Antworten des Auftragsverarbeiters verlassen und bekommt keinen eigenen Einblick in den tatsächlichen Ist-Zustand. Somit besteht die Problematik eingeschränkt valider Ergebnisse und damit dem Fehlen einer substanziellen Entscheidungsgrundlage für das weitere Vorgehen mit dem jeweiligen Auftragsverarbeiter.

Für die gesetzeskonforme Durchsetzung des Rechts auf Löschung konnten durch die vorhandene Literatur und eigene Überlegungen geeignete Lösungen und Handlungsempfehlungen für die Praxis abgeleitet werden. Durch die Trennung der Löschung im Zusammenhang mit Löschbegehren betroffener Personen und der Löschung aus den in Art. 17 Abs. 1 lit. a) – f) DS-GVO genannten Gründen konnten klare und eindeutige Prozesse definiert werden. Dabei hat sich gezeigt, dass verständliche und unmittelbar geltende Anweisungen der beteiligten Mitarbeiter unausweichlich sind, um den Ablauf dieser Prozesse sicherzustellen. Die erkannte, teilweise fehlende Aufmerksamkeit und das fehlende Bewusstsein innerhalb eines Unternehmens kann durch Schulungen erhöht werden. Durch die Festlegung der Verantwortlichkeiten anhand von Rollen und Positionen konnte zudem eine höhere Prozessstabilität sowie eine Vereinfachung der einzelnen Schritte wie dem Identifizieren personenbezogener Daten in sämtlichen Systemen erreicht werden. Darüber hinaus werden durch dieses Vorgehen die Dokumentations- und Nachweispflichten des Verantwortlichen erfüllt. Somit kann eine Implementierung dieses Löschkonzepts helfen, den Herausforderungen entgegenzutreten und gemäß den gesetzlichen Anforderungen zu agieren.

Die praktischen Problemstellungen mit Blick auf die Kontrolle der TOMs bei Auftragsverarbeitern konnten durch die Kombination verschiedener Methoden gelöst werden. Die Anwendung von Fragebögen bzw. Checklisten als Basis der Kontrolle und einer nachfolgenden Vor-Ort-Kontrolle hat sich als vorteilhaft erwiesen. Den begrenzten personellen und wirtschaftlichen Möglichkeiten vieler Unternehmen kann durch die ausschließliche Einzelfallanwendung der aufwandsintensiven Vor-Ort-Kontrolle Rechnung getragen werden. Gleichzeitig kann dadurch eine hohe Validität der Ergebnisse sichergestellt werden. Wie sich herausstellte wird den Zertifizierungen gemäß Art. 42 f. DSGVO in der betrieblichen Praxis bisher noch keine entscheidende Bedeutung zugeschrieben. Jedoch kann ein solches Zertifikate als zusätzliches Indiz für das Vorliegen geeigneter TOMs herangezogen werden. Somit wurde eine aussagekräftige Bewertungsgrundlage bezüglich des weiteren Vorgehens mit den entspre-

chenden Dienstleistern geschaffen. Durch dieses Vorgehen kann der Aufwand reduziert werden, was zu geringeren Kosten führt. Durch den effizienten Prozess und den abschließend zur Verfügung gestellten Prüfbericht kann eine wirtschaftliche Möglichkeit zur rechtmäßigen und turnusmäßigen Überprüfung der TOMs aufgezeigt werden.

Im Hinblick auf die rasante datenschutzrechtliche Entwicklung, insbesondere hinsichtlich der Verarbeitung personenbezogener Daten und die fortwährende Weiterentwicklung technischer Möglichkeiten müssen die Konzepte und Vorgehensweisen stets auf dem aktuellen Stand gehalten werden und auf individuelle Unternehmensstrukturen angepasst sein. Die entwickelten Methoden können bei solchen Änderungen oder neuen Rechtsprechungen leicht angepasst werden. Die Wichtigkeit dieser Themen wurde mittlerweile in allen Bereichen erkannt. Bei der Entwicklung neuer datenverarbeitender Systeme wird von den Herstellern in Zukunft mehr auf die Möglichkeit der Identifizierung und Löschung personenbezogener Daten geachtet werden. Dies kann zusätzlich zur Vereinfachung der Löschung personenbezogener Daten beitragen. Das gestiegene Bewusstsein kann sich bei den Auftragsverarbeiten auch auf die Kontrolle der TOMs und somit durch wahrheitsgemäße Antworten auf den Kontrollaufwand auswirken. Durch die aufgezeigten Konzepte und Abläufe auch aus Literatur und durch die Behörden können die datenschutzrechtlichen Vorschriften bei Weiterentwicklungen und Veränderungen im rechtlichen oder technischen Bereich weiterhin im höchstmöglichen Maße erfüllt werden.

7 LITERATURVERZEICHNIS

Art. 29 – Datenschutzgruppe: WP 136. Begriff der personenbezogenen Daten, URL: https://datenschutz.hessen.de/infothek/europäischer-datenschutzausschuss-artikel-29-datenschutzgruppe, Abruf: 24.09.2020

Art. 29 – Datenschutzgruppe: WP 168. Die Zukunft des Datenschutzes – gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten, URL: https://www.bfdi.bund.de/SharedDocs/Publikationen/EU/Art29Gruppe/WP168_de.html?cms_submit=Senden&cms_templateQueryString=wp+168, Abruf: 05.10.2020

Art. 29 – Datenschutzgruppe: WP 169 Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, URL: https://ec.europa.eu/justice/ article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf, Abruf: 22.10.2020

Art. 29 – Datenschutzgruppe: WP 216 Stellungnahme 5/2014 zu Anonymisierungstechniken, URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf, Abruf: 10.12.2020

Auer-Reinsdorff, Astrid; Conrad Isabell: *Handbuch IT- und Datenschutzrecht*, 3. Auflage, C.H. Beck, München 2019

Baumgartner, Ulrich; Gausling, Tina: „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“, in: *Zeitschrift für Datenschutz*, 07/2017

Bechtolt, Hans; Vogt, Niklas: „Datenschutz in der Blockchain – Eine Frage der Technik“, in: *Zeitschrift für Datenschutz*, 02/2018

Berliner Beauftragte für Datenschutz und Informationsfreiheit: Pressemitteilung 711.412.1 v. 05.11.2019

Berning, Wilhelm; Keppeler, Lutz Martin: „Technische und rechtliche Probleme bei der Umsetzung der DS-GVO Löschpflichten“, in: *Zeitschrift für Datenschutz*, 07/2017

Bitkom e. V.: Begleitende Hinweise zu der Anlage Auftragsverarbeitung – Leitfaden, URL: https://www.bitkom.org/sites/default/files/file/import/170515-LF-Auftragsverarbeitung-online.pdf, Abruf: 20.10.2020

Bitkom e.V.: DS-GVO, ePrivacy, Brexit – Datenschutz und die Wirtschaft, URL: https://www.bitkom.org/sites/default/files/2019-09/bitkom-charts-pk-privacy-17- 09-2019.pdf, Abruf: 16.09.2020

Bogner, Alexander; Littig, Beate; Menz, Wolfgang: „Interviews mit Experten - Eine praxisorientierte Einführung“, in: Bohnsack, Ralf; Flick, Uwe; Lüders, Christian; Reichertz, Jo (Hrsg.): *Qualitative Sozialforschung*, Springer Fachmedien, Wiesbaden 2014

Brink, Stefan: Der Landesbeauftragte, URL: https://www.baden-wuerttemberg.datenschutz.de/der-landesbeauftragte-fuer-den-datenschutz-und-die-informationsfreiheit-baden-wuerttemberg, Abruf: 14.09.2020

Brink, Stefan; Eckhardt, Jens: „Wann ist ein Datum ein personenbezogenes Datum? Anwendungsbereich des Datenschutzrechts“, in: *Zeitschrift für Datenschutz*, 05/2015

Brink, Stefan; Wolff, Heinrich Amadeus (Hrsg.): *BeckOK Datenschutzrecht*, 33. Edition, C.H. Beck, München 2020

Buchner, Benedikt; Kühling, Jürgen (Hrsg.): *Datenschutz-Grundverordnung / BDSG*, 2. Aufl., C.H. Beck, München 2018

Bundesamt für die Sicherheit in der Informationstechnik: Daten richtig löschen, URL: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/richtigloeschen_node. html, Abruf: 14.10.2020

Datenschutzkonferenz: Kurzpapier Nr. 6 Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO, URL: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf, Abruf: 15.12.2020.

Datenschutzkonferenz: Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, URL: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf, Abruf: 21.10.2020

Der Bayerische Landesbeauftragte für den Datenschutz: Aktuelle Kurz-Information 6 - Keine gesonderte Entgeltpflicht für Kontrollen bei der Auftragsverarbeitung, URL: https://www.datenschutz-bayern.de/datenschutzreform2018/aki06.pdf

Der Bayerische Landesbeauftragte für den Datenschutz: Arbeitspapier zur Zertifizierung – Art. 42 DS-GVO, URL: https://www.lda.bayern.de/media/baylda_ds-gvo_2_certification.pdf, Abruf 18.11.2020

Der Bayerische Landesbeauftragte für den Datenschutz: Auftragsverarbeitung - Orientierungshilfe, URL: https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf, Abruf 23.09.2020

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg: Tätigkeitsbericht 2018, URL: https://www.baden-wuerttemberg.datenschutz.de/wp-

content/uploads/2019/02/LfDI-34.-Datenschutz-Tätigkeitsbericht-Internet.pdf, Abruf: 14.09.2020

Die Landesbeauftragte für den Datenschutz Niedersachsen: Querschnittsprüfung Abschlussbericht November 2019, URL: https://lfd.niedersachsen.de/download/14930, Abruf 16.09.2020

Ebert, Nico; Knuchel, Christian: "DSGVO-konformes Löschen – Ein Praxisbericht zur Umsetzung von Artikel 17 bei der AXA Schweiz AG", in: *Datenschutz und Datensicherheit*, 02/2020

Eckhardt, Jens: DS-GVO: „Anforderungen an die Auftragsverarbeitung als Instrument zur Einbindung Externer", in: *Corporate Compliance Zeitschrift*, 03/2017

Ehmann, Eugen; Selmayr, Martin (Hrsg.): *DS-GVO*, 2. Aufl., C.H. Beck, München 2018

European Commission: Adequacy decisions, URL: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy- decisions_en, Abruf 18.09.2020

European Data Protection Board: EDPB & EDPS adopt joint opinions on new sets of SCCs, URL: https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinions-new-sets-sccs_en, Abruf: 19.01.2021

Forgó, Nikolaus; Helfrich, Marcus; Schneider, Jochen (Hrsg.): *Betrieblicher Datenschutz. Rechtshandbuch*, 3. Aufl., C.H. Beck, München 2019

Gola, Peter (Hrsg.): *Datenschutz-Grundverordnung*, 2. Aufl., C.H. Beck, München 2018

Gürtler, Paul: „Praxisfragen der Auftragsverarbeitung", in: Zeitschrift für Datenschutz, 02/2019

Hammer, Volker: DIN 66398 - Die Leitlinie Löschkonzept als Norm, in: *Datenschutz und Datensicherheit*, 08/2016

Hammer, Volker; Schuler, Karin: DIN - Deutsches Institut für Normung e.V. - "Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten", URL: https://www.secorvo.de/publikationen/din-leitlinie-loeschkonzept-hammer-schuler-2012.pdf, Abruf 05.11.2020

Hanschke, Inge: *Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten – Eine kompakte Einführung in die Praxis*, 2. Auflage, Springer, Wiesbaden 2020

Härting, Niko: Datenschutz-Grundverordnung: *Das neue Datenschutzrecht in der betrieblichen Praxis*, 1. Aufl., Verlag Dr. Otto Schmidt 2016

Hartung, Jürgen; Büttgen, Lisa: „Die Auftragsverarbeitung nach der DS-GVO", in: *Datenschutz und Datensicherheit*, 09/2017

Hennemann, Moritz: „Das Recht auf Löschung gemäß Art. 17 Datenschutz-Grundverordnung", in: *PinG*, 05/2016

Herfurth, Constantin: „Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO", in: *Zeitschrift für Datenschutz*, 11/2018

Ingelheim, Alexander: „Das erste Jahr DSGVO - Eine Bestandsaufnahme", in: Controling & Management Review 63, 04/2019

Jaspers, Andreas; Jacquemain, Tobias: „Datenschutz-Grundverordnung – Praxiserfahrungen und Evaluation Aus der Sicht von Datenschutzbeauftragten“, in: Datenschutz und Datensicherheit, 05/2020

Jung, Alexander: „Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO“, Zeitschrift für Datenschutz, 05/2018

Knoll, Mathias; Strahringer, Susanne (Hrsg.): IT-GRC-Management – Governance, Risk und Compliance Grundlagen und Anwendungen, 1. Aufl., Springer, Wiesbaden 2017

Lachenmann, Matthias; Koreng, Ansgar (Hrsg.): Formularhandbuch Datenschutzrecht, 2.Aufl., C.H. Beck, München 2018

Laue, Philip, Kremer, Sascha (Hrsg.): Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl., Nomos, Baden-Baden 2019

Martini, Mario; Weinzierl, Quirin: „Die Blockchain-Technologie und das Recht auf Vergessenwerden: zum Dilemma zwischen Nicht-Vergessen-Können und Vergessen-Müssen“, in: NvWZ, 17/2017

Mühlbauer, Holger: EU-Datenschutz-Grundverordnung (DSGVO) – Praxiswissen für die Umsetzung im Unternehmen – Schnellübersichten, 2. Auflage, Beuth Verlag, Berlin 2018

Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 2. Aufl., C.H. Beck, München 2018

Plath, Kai-Uwe (Hrsg.): DSGVO/BDSG, 3. Aufl., Otto Schmidt, Köln 2018

Reiners, Wilfried: Datenschutz in der Personal Data Economy – Eine Chance für Europa, in: Zeitschrift für Datenschutz, 02/2015

Richter, Frederick: „Zertifizierung unter der DS-GVO - Chance eines erleichterten internationalen Datenverkehrs darf nicht verpasst werden“, in: Zeitschrift für Datenschutz, 02/2020

Roßnagel, Alexander: Das neue Datenschutzrecht. Europäische Datenschutz- Grundverordnung und deutsche Datenschutzgesetze, Nomos, Baden-Baden 2018

Roßnagel, Alexander: „Datenschutzgrundsätze – unverbindliches Programm oder verbindliches Recht? Bedeutung der Grundsätze für die datenschutzrechtliche Praxis“, in: Zeitschrift für Datenschutz, 08/2018

Roßnagel, Alexander: „Evaluation der Datenschutz-Grundverordnung Verfahren – Stellungnahmen – Vorschläge“, in: Datenschutz und Datensicherheit, 05/2020

Roßnagel, Alexander: „Evaluation nutzen!“, in: Datenschutz und Datensicherheit, 05/2020

Roßnagel, Alexander; Nebel, Maxi; Richter, Philipp: „Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO“, in: Zeitschrift für Datenschutz, 10/2015

Roßnagel, Alexander: „Pseudonymisierung personenbezogener Daten. Ein zentrales Instrument im Datenschutz nach der DS-GVO“, in: *Zeitschrift für Datenschutz*, 06/2018

Schäfer, Christoph; Fox, Dirk: „Zertifizierte Auftragsdatenverarbeitung - Das Standard- ADV-Modell“, in: *Datenschutz und Datensicherheit*, 11/2016

Schneider, Jochen: *Datenschutz nach der EU-Datenschutz-Grundverordnung*, 2. Aufl., C.H. Beck, München 2019

Schröder, Markus: „Der risikobasierte Ansatz in der DS-GVO - Risiko oder Chance für den Datenschutz?“, in: *Zeitschrift für Datenschutz*, 11/2019

Schulz, Sebastian: „Die Evaluation der DSGVO - Anregungen aus dem Maschinenraum“, in: *Datenschutz und Datensicherheit*, 05/2020

Schwartmann, Rolf; Jaspers, Andreas; Thüsing, Gregor; Kugelmann, Dieter (Hrsg.): *DS-GVO/BDSG. Datenschutz-Grundverordnung. Bundesdatenschutzgesetz*, C.F. Müller, Heidelberg 2018

Simitis, Spiros; Hornung, Gerrit; Spiecker, Indra (Hrsg.): *Datenschutzrecht. DSGVO mit BDSG*, Nomos, Baden-Baden 2019

Specht, Louisa; Mantz, Reto (Hrsg.): *Handbuch Europäisches und deutsches Datenschutzrecht*, 1. Aufl., C.H. Beck, München 2019

Sydow, Gernot: *Europäische Datenschutzgrundverordnung*, 2. Aufl., Nomos, Baden-Baden 2018

Tinnefeld, Marie-Theres; Buchner, Benedikt; Petri, Thomas; Hof, Hans-Joachim: *Einführung in das Datenschutzrecht*, 7. Aufl., De Gruyter, Oldenbourg 2020

TÜV Süd AG: ISO/IEC 27001 - ISMS-ZERTIFIZIERUNG, URL: https://www.tuvsud.com/de-de/dienstleistungen/auditierung-und-zertifizierung/cyber-security-zertifizierung/iso-27001, Abruf: 23.11.2020

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Hinweise zur Dokumentation einer ordnungsgemäßen Verarbeitung personenbezogener Daten, URL: https://www.datenschutzzentrum.de/uploads/dokumentation/Hinweise_zur_Dokumentation.pdf, Abruf: 08.01.2021

Voigt, Paul; von dem Bussche, Axel: *EU-DatenschutzGrundverordnung (DSGVO) Praktikerhandbuch*, Springer, Wiesbaden 2018

Voigt, Paul; von dem Bussche, Axel (Hrsg.): *Konzerndatenschutz. Rechtshandbuch*, 2. Aufl., C.H. Beck, München 2019

Wächter, Michael: *Datenschutz im Unternehmen*, 5. Auflage, C.H. Beck, München 2017

Weichert, Thilo: „Die DSGVO, ein – ganz guter – Anfang“, in: *Datenschutz und Datensicherheit*, 05/2020

Wennemann, Thomas: „TOM und die Datenschutz-Grundverordnung“, in: *Datenschutz und Datensicherheit*, 01/2018

Wichtermann, Marco: Einführung eines Datenschutz-Management-Systems im Unternehmen – Pflicht oder Kür? Kurzüberblick über die Erweiterungen durch die DS-GVO, in: *Zeitschrift für Datenschutz*, 09/2016

8 AUTORENINFORMATION

Alexander Steinhart, LL.M., ist Absolvent des Masterstudienganges Legal Management (WRM) an der Hochschule Konstanz.

Dr. Thomas Zerres ist Professor für Zivil- und Wirtschaftsrecht an der Hochschule Konstanz. Vor seinem Ruf an die Hochschule Konstanz lehrte Prof. Dr. Thomas Zerres 15 Jahre an der Hochschule Erfurt, nachdem er mehrere Jahre als Rechtsanwalt und als Bundesgeschäftsführer eines großen Wirtschaftsverbandes der Dienstleistungsbranche tätig war. Seine Lehr- und Forschungsschwerpunkte sind das Marketingrecht sowie das Europäische Privatrecht.

Dr. Christopher Zerres ist Professor für Marketing an der Hochschule Offenburg. Seine Schwerpunkte in Lehre und Forschung liegen auf dem Online-Marketing und dem Marketing-Controlling. Christopher Zerres ist Autor zahlreicher Publikationen zu den Bereichen Management und Marketing.