Avdimetaj, Valona; Loomans, Dirk; Zerres, Thomas

Working Paper

Plädoyer für eine stärkere Berücksichtigung des Datenschutzes in der ESG-Dimension

Arbeitspapiere für Marketing und Management, No. 67

Provided in Cooperation with:
Fakultät Medien, Hochschule Offenburg

Suggested Citation: Avdimetaj, Valona; Loomans, Dirk; Zerres, Thomas (2022) : Plädoyer für eine stärkere Berücksichtigung des Datenschutzes in der ESG-Dimension, Arbeitspapiere für Marketing und Management, No. 67, Hochschule Offenburg, Fakultät Medien, Offenburg, https://doi.org/10.48584/opus-6264

This Version is available at:
https://hdl.handle.net/10419/266632

CHRISTOPHER ZERRES

MARKETING

Schriftenreihe „Arbeitspapiere für Marketing und Management“

Herausgeber:
Prof. Dr. Christopher Zerres

Hochschule Offenburg
Fakultät Medien

Arbeitspapier Nr. 67

Plädoyer für eine stärkere Berücksichtigung des Datenschutzes in der ESG-Dimension

Avdimetaj, V., Loomans, D., Zerres, T.

Offenburg, November 2022

ISSN: 2510-4799

Impressum

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

ISSN: 2510-4799

Inhalt

1 EINFÜHRUNG

Initiativen wie „Fridays for Future“ und die Veröffentlichung des europäischen Grünen Deals am 11.12.2019[1] rücken die Aspekte ökologische Nachhaltigkeit und unternehmerische Sozialverantwortung immer stärker in den Fokus von potenziellen Anlegern und bilden eine fundamentale Grundlage von Investitionsentscheidungen.[2] Viele Anleger verfolgen dabei nicht mehr ausschließlich monetäre oder renditemaximierende Ziele, sondern erwägen auch soziale und ökologische Konsequenzen ihrer Investitionen. Ursprung des Drucks, welcher durch die oben genannten Stakeholder verstärkt ausgeübt wird, sind jedoch vielmehr die aus dem Klimawandel resultierenden Naturkatastrophen und die damit einhergehenden Schäden.[3] Vor diesem Hintergrund wurden die drei Säulen Environmental, Social und Governance (im Folgenden „ESG“) ins Leben gerufen, welche zu einer der größten Entwicklungen des Finanzmarktes in den letzten Jahren zählen.[4] Dabei spiegelt sich die immer mehr zunehmende Relevanz in dem exponentiellen Anstieg der ESG-Investitionen wider. Die Global Sustainable Investment Alliance verzeichnet für das Jahr 2020 Investitionen von etwa 35 Billionen US-Dollar, die auf den drei Kriterien basieren und erleben damit einen Anstieg von über 15% innerhalb von zwei Jahren und sogar einen Anstieg von über 55% seit 2016 .[5] In Europa wird dies insbesondere durch die Legislative in Form von Gesetzen wie etwa die delegierte Verordnung für EU-Taxonomie[6], die 2020 in Kraft trat oder die seit März 2022 rechtsverbindliche EU-Offenlegungsverordnung[7] getrieben[8].

In diesem Zusammenhang ist jedoch die zunehmende Bedeutung des Datenschutzes seit Inkrafttreten der Datenschutzgrundverordnung[9] (im Folgenden „DSGVO“) nicht zu verkennen, die sich sowohl anhand der Menge zu verarbeitender Daten als auch an der Höhe der Bußgelder erkennen lässt. 2020 erreichte das Volumen der zu verarbeitenden Daten einen Umfang von über 50 Zetabyte.[10] Bis 2025 soll Experten zufolge die weltweite Datenmenge auf 175 Billionen Gigabyte steigen[11], was naturgemäß auch mit einer größeren Menge personenbezogener Daten i.S.d. DSGVO einhergeht. Daneben haben die verhängten Bußgelder erst im vergangenen Jahr die Milliardengrenze überschritten und be-

[1] Vgl. *Europäische Kommission* (Hrsg.), Der europäische Grüne Deal, 11.12.2019.
[2] Vgl. *CFA Institute Research Foundation (Hrsg.)*, ESG and Responsible Institutional Investing Around the World – A Critical Review, S. 1.
[3] Vgl. *Europäische Kommission (Hrsg.),* Folgen des Klimawandels.
[4] Vgl. *Christensen/Serafeim/Sikochi*, Why is Corporate Virtue in the Eye of The Beholder? The Case of ESG Rating, S. 1.
[5] Vgl. *Global Sustainable Investment Alliance (Hrsg.),* Global Sustainable Investment Review 2020, S. 9.
[6] Vgl. Verordnung (EU) 2019/2088 des Europäischen Parlaments und des Rates vom 27. November 2019 über nachhaltigkeitsbezogene Offenlegungspflichten im Finanzdienstleistungssektor (Text von Bedeutung für den EWR).
[7] Vgl. Verordnung (EU) 2019/2088 des Europäischen Parlaments und des Rates vom 27. November 2019 über nachhaltigkeitsbezogene Offenlegungspflichten im Finanzdienstleistungssektor.
[8] Vgl. *Europäische Kommission (Hrsg.)*, Gerechte und nachhaltige Wirtschaft: Kommission legt Unternehmensregeln für Achtung der Menschenrechte und der Umwelt in globalen Wertschöpfungsketten fest.
[9] Vgl. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden: Datenschutz-Grundverordnung).
[10] Vgl. *Bundesministerium für Wirtschaft und Klimaschutz (Hrsg.)*, Datenökonomie.
[11] Vgl. *Networkworld (Hrsg.)*, IDC: Expect 175 zettabytes of data worldwide by 2025.

laufen sich insgesamt auf ca. 1,3 Milliarden Euro; somit erleben die Bußgelder einen Anstieg von über 740% im Gegensatz zum Vorjahr.[12] Die Folgen aus einem Verstoß gegen die DSGVO sind dabei nicht nur per se monetärer Natur, sondern wirken sich sowohl auf die Reputation als auch auf den Unternehmenswert aus. Dies wurde unlängst am Beispiel von WhatsApp deutlich, als mit Ankündigung einer intransparenten Datenschutzrichtlinie der unmittelbare Konkurrent Telegram, parallel zu jenem Ereignis, einen Zuwachs von fast 25 Millionen Nutzern innerhalb von 72 Stunden erfuhr.[13] Dieses Beispiel verdeutlicht, dass die Missachtung des Datenschutzes eine weitaus größere Tragweite als lediglich datenschutzrechtliche Sanktionen und Bußgelder hat. Anlässlich dessen ist es von großer Bedeutung, Unternehmen in die Lage zu versetzen, die eigenen Datenschutzrisiken zu identifizieren, zu verstehen und ggf. zu minimieren, um diese daraufhin den Stakeholdern wie etwa der Geschäftsleitung, Geschäftspartnern, Kunden und Aufsichtsbehörden zu erläutern.[14]

1.1 Begründung des Forschungsproblems und Zielsetzung

Die Problemstellung, die diesem neuen Arbeitspapier zugrunde liegt, ist die Kritik an der bisherigen Etablierung des Datenschutzes in der ESG-Dimension und die Berücksichtigung dessen in dem ESG-Score, welcher eine grundlegende Orientierung für Investitionsentscheidungen von ESG-Anlegern darstellt. Dabei wird verkannt, dass der Datenschutz vieldimensionale Implikationen birgt und somit ebenfalls als ein Nachhaltigkeitsthema verstanden werden kann. Dies ist auch Anlass für die aktuell herrschende Uneinigkeit über die dezidierte Kategorisierung des Datenschutzes in eine der drei Säulen.[15] Während sich jedoch die Wettbewerbsteilnehmer dem gesellschaftlichen Anspruch nach mehr Umweltschutz beugen und daher umweltfreundlichere Güter entwickeln sowie produzieren, bleiben dabei die datenschutzrechtlichen Anforderungen in vielen Fällen unberücksichtigt.[16] Die Wurzeln dieser Problematik könnten darin liegen, dass der Datenschutz immer noch als ein isoliertes Themengebiet behandelt wird, das für viele als Hindernis für Innovation und Digitalisierung gilt.[17] Daneben aber auch darin, dass der ökologischen Nachhaltigkeit aufgrund der unmittelbaren monetären Konsequenzen z.B. in Form der CO2-Steuer mehr Achtung gewidmet wird.[18] Des weiteren steht eine saubere Umwelt im kausalen Zusammenhang zu den menschlichen Bedürfnissen und gilt als „moralischer und ökonomischer Imperativ des 21. Jahrhunderts“[19].[20] Zum einen lastet zwar der Druck der Gesellschaft und die öffentliche Präsenz der ökologischen Nachhaltigkeit auf den Schultern der Unternehmen, zum anderen treiben u.a. Organisationen wie NOYB[21] das

[12] Vgl. *Statista (Hrsg.)*, DSGVO-Bußgelder knacken 2021 die Milliardengrenze.
[13] Vgl. *Funkschau (Hrsg.)*, der mündige (gläserne) Nutzer?.
[14] Vgl. *A&M*, ESG and Privacy – a Foundation for Better Compliance?.
[15] Vgl. *Collyer Bristow (Hrsg.)*, ESG and Data Protection; *Dein Geld anlegen (Hrsg.)*, ESG Ratings – Übersicht: Welche gibt es?, im Rahmen der Aufführung der ESG-Kriterien ordnet MSCI Datenschutz in die Social-Säule ein.
[16] Vgl. *Basecamp (Hrsg.)*, Nachhaltigkeit und Datenschutz – Neues von der CDR-Initiative; *Handelsblatt (Hrsg.)*, Mangelnder Datenschutz: Justizministerium lehnt Scheuers Gesetz zum autonomen Fahren ab.
[17] Vgl. *Handelsblatt (Hrsg.)*, Mangelnder Datenschutz: Justizministerium lehnt Scheuers Gesetz zum autonomen Fahren ab.
[18] Vgl.*Wirtschaftswoche (Hrsg.)*, CO2-Steuer in Deutschland – Kosten, Berechnung und Co. – alles, was Sie wissen müssen.
[19] *Dörr*, Praxisleitfaden Corporate Digital Responsibility, S. 2.
[20] *Gruenderfreunde (Hrsg.)*, Was ist Nachhaltigkeit?; *Dörr*, Praxisleitfaden Corporate Digital Responsibility, S. 2.
[21] Vgl.*NOYB (Hrsg.)*, NOYB enforces your right to privacy everyday.

Thema Datenschutz immer stärker in den Vordergrund. Denn die rasant steigende Digitalisierung und die Zunahme der verarbeitenden Daten lassen den Ruf nach nachhaltigem Umgang mit (personenbezogenen) Daten laut werden. Als Folge daraus entstehen zwischen den ergriffenen ESG-Maßnahmen Kollisionen und damit den einzelnen Säulen, die ein Spannungsfeld in der gesamten Ära verursachen. Die Frage, die daher hier zu beantworten ist, ist, ob dem ökologischen Nachhaltigkeitsgedanken und damit dem „E" der drei Säulen Vorrang gewährt werden kann, sodass weitere Nachhaltigkeitskriterien wie bspw. der nachhaltige Umgang mit Daten diesem untergeordnet werden und inwiefern dies gerechtfertigt ist. Es bleibt also zu eruieren, ob der Nachhaltigkeitsaspekt zu Lasten der anderen ESG-Elemente verfolgt werden kann und ob dies nicht vielmehr zu einem Ungleichgewicht führt. Entsprechend der gesellschaftlichen Nachfrage richten ESG-Rating-Agenturen aufgrund der oben genannten Tatsachen bei der Berechnung der ESG-Ratings ihren Fokus insbesondere auf die ökologische Nachhaltigkeit, wie der ersten Abbildung zu entnehmen ist.[22]

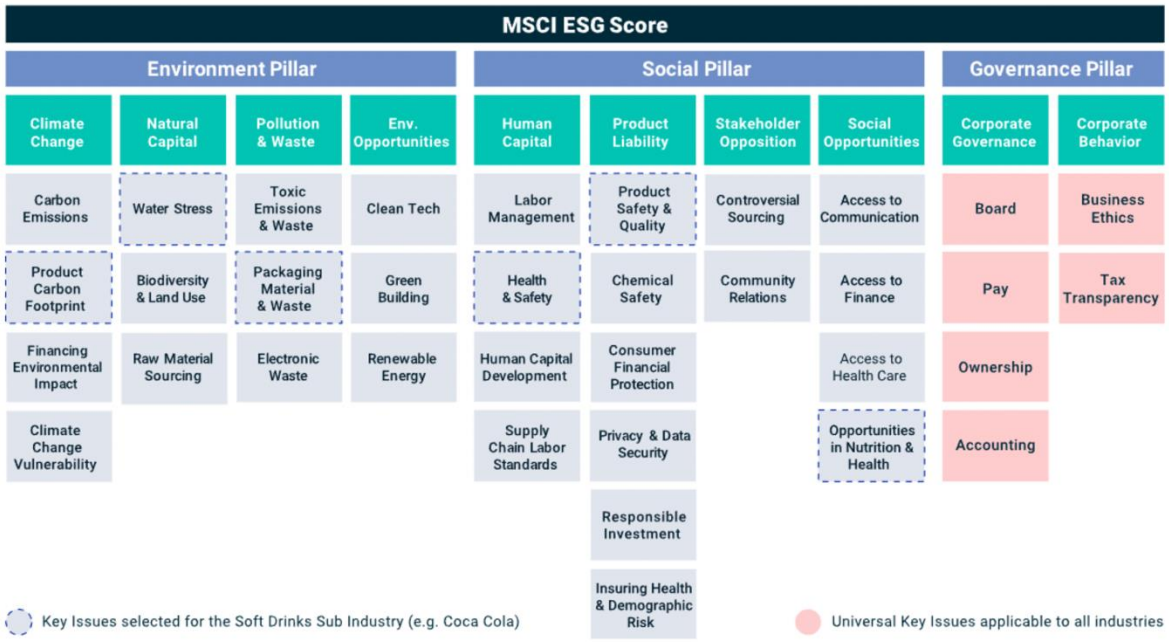

Abbildung 1: ESG Rating & Agenturen Übersicht.

Dein Geld anlegen (Hrsg.), ESG Ratings - Übersicht: Welche gibt es?, online abrufbar unter: https://www.dein-geld-anlegen.de/esg-rating-agenturen-uebersicht/, zuletzt besucht am 28.09.2022.

In Anbetracht der zunehmenden Bedeutung des Datenschutzes, scheinen somit auch ESG-Ratings von Ratingagenturen wie bspw. das der MSCI (Morgan Stanley Capital Internationals) überholt zu sein und müssen auf diesen Umstand hin reformiert werden. Die Akzeptanz des Datenschutzes als ethische Selbstverpflichtung und damit als Nachhaltigkeitsaspekt postuliert die Einbettung des Datenschutzes in die Unternehmensstrategien. Mangels eindeutiger gesetzlicher Vorgaben, Richtlinien und/oder Orientierungshilfen besteht für Unternehmen künftig die Schwierigkeit darin, eine Datenschutz-Strategie zu entwickeln und diese umzusetzen. Es besteht somit der Bedarf, den Unternehmen Vorgaben zur Verfügung zu stellen, die eine Strategiedefinition und -umsetzung ermöglichen in Begleitung von Beratern.

[22] Vgl. *MSCI (Hrsg.)*, MSCI ESG Government Ratings, S. 10.

1.2 AUFBAU

Aus den oben genannten Missständen wird deutlich, dass der Datenschutz in einem Konflikt mit allen drei Dimensionen steht, insofern er nicht ebenfalls als integraler Bestandteil der ESG-Ära akzeptiert wird. Ziel ist es daher, dass der nachhaltige Umgang mit Daten ebenso Akzeptanz als Teil dieser Materie findet, sodass das Gleichgewicht wieder hergestellt und damit ein Ausgleich geschaffen werden kann. Mit Hinblick auf die Schwierigkeit der Zuordnung des Datenschutzes im ESG-Kontext wird im ersten Schritt der Ursprung und der Zweck der DSGVO beleuchtet, um anschließend eine dezidierte Kategorisierung des Datenschutzes in eines der drei ESG-Paradigmen vorzunehmen. Diverse Praxisbeispiele zeigen ferner auf, welche Implikationen der Schutz von personenbezogenen Daten auf die ESG-Dimensionen hat und wie dadurch Spannungsverhältnisse entstehen. Darauffolgend werden datenschutztechnische Lösungsmöglichkeiten erörtert mit dem Ziel, eine Balance zu schaffen und diese Spannungsverhältnisse zu lösen. Sodann folgt eine Untersuchung, ob der Datenschutz den erforderlichen Materialisierungsgrad erfüllt, um in ESG-Ratings adäquat berücksichtigt werden zu können. Daraufhin wird das MSCI ESG Scoring kritisch im Hinblick auf den Datenschutz analysiert. Das Spektrum der ESG-Ratings inkludiert neben der Bewertung von Unternehmen auch das Erstellen von Produkt- und Länderscores, die jedoch nicht im Hauptaugenmerk dieses Arbeitspapiers liegen. Das letzte Kapitel zeigt auf, wie eine ESG-Strategie unter Hinzuziehung des Datenschutzes aussehen kann und wie die Beratung vor diesem Hintergrund ausgestaltet wird. Als Teil der Strategieumsetzung erfolgt eine detaillierte Beschreibung des Datenschutzrisikomanagements.

2 ENVIRONMENTAL, SOCIAL UND GOVERNANCE UND DIE VERORTUNG DES DATENSCHUTZES

2.1 BEGRIFFSDEFINITIONEN UND -ABGRENZUNG

2.1.1 Definition der Nachhaltigkeit

Der Begriff der Nachhaltigkeit hat seinen Ursprung im Mittelalter und entstand aus der Forstwirtschaft. Hans Carl von Carlowitz, der Erschaffer des Begriffs der Nachhaltigkeit, griff in seiner Pionierarbeit „Sylvicultura oeconomica“ von 1713 den Grundgedanken auf, innerhalb einer Periode nicht mehr Holz zu fällen, als im gleichen Zeitraum durch Aufforstung nachwachsen kann.[23] In Ermangelung einer einheitlichen Definition greift die Praxis auf die gängige Begriffserklärung des Brundtland-Berichts der Vereinten Nationen aus dem Jahre 1987 zurück. Nach dieser versteht man unter der nachhaltigen Entwicklung Folgendes: *„Sustainable development is development that meets the needs of the present without compromising the ability of future generations to meet their own needs“.*[24] Gemäß dieser Definition muss die Befriedigung von Bedürfnissen in der Gegenwart in der Weise erfolgen, ohne dass künftige Generationen in der Befriedigung deren eigener Bedürfnisse beeinträchtigt werden. Der Rat für Nachhaltige Entwicklung konkretisiert den Begriff und versteht darunter die gleichberechtigte Berücksichtigung mit sozialen und wirtschaftlichen Gesichtspunkten von Umweltaspekten.[25] Ferner erklärt dieser zukunftsfähiges Wirtschaf-

[23] Vgl. *Grober*, Die Entdeckung der Nachhaltigkeit: Kulturgeschichte eines Begriffs, S. 116.
[24] *United Nations (Hrsg.)*, Our Common Future: Report of the World Commission on Environment and Development, S. 17.
[25] Vgl. *Rat für nachhaltige Entwicklung (Hrsg.)*, Nachhaltige Entwicklung.

ten wie folgt: „Wir müssen unseren Kindern und Enkelkindern ein intaktes ökologisches, soziales und ökonomisches Gefüge hinterlassen. Das Eine ist ohne das Andere nicht zu haben."[26] Das Konzept der Nachhaltigkeit basiert daher auf dem sog. Tripple-Bottom-Line-Ansatz (Abbildung 2). Danach sind Wirtschaft, Ökologie und Soziales **gleichrangig und gleichgewichtig**, und zwar sowohl auf gesamtwirtschaftlicher und politischer Ebene, als auch auf globaler und unternehmerischer Ebene.[27] Aus der Abbildung geht hervor, dass nicht nur die klassische rein wirtschaftliche Leistung von Bedeutung ist, sondern dass Unternehmen auch soziale und ökologische Ziele verfolgen müssen. Zu beachten ist jedoch, dass soziale und ökologische Aktivitäten stets wirtschaftlich sinnvoll sein und einen Beitrag zum ökonomischen Ziel leisten müssen, um die Wirtschaftlichkeit der Institution zu gewährleisten.[28]

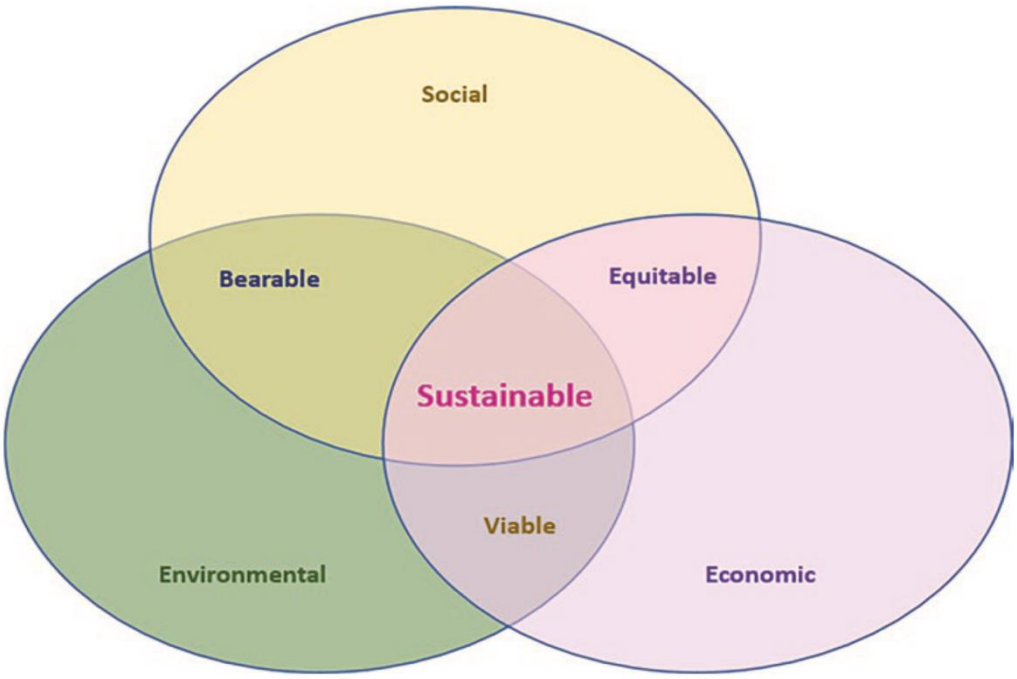

Abbildung 2: Die drei Säulen der Nachhaltigkeit.

Elkington (Hrsg.), Cannibals with forks: The triple bottom line of 21st century business.

2.1.2 Environmental, Social und Governance

So wie beim Begriff der Nachhaltigkeit mangelt es auch für ESG an einer allgemeingültigen Definition, da die drei Paradigmen mitunter subjektiven Faktoren unterliegen. Die Abkürzung ESG steht für Environmental (Umwelt), Social (Soziales) und Governance. (Unternehmensführung). Eine anerkannte Definition von ESG lautet: „ESG-Investitionen sind ein Research- und Anlagestrategierahmen, der Umwelt-, Sozial- und Governance-Faktoren als nicht-finanzielle Dimensionen der Bewertung, der Performance und des Risikoprofils eines Wertpapiers bewertet."[29] Der Begriff wird somit vor allem im Zusammenhang mit Investments verwendet, um zu evaluieren, ob und inwiefern Unternehmen den Anforderungen an Nachhaltigkeit hinsichtlich der drei Bereiche Umwelt, Soziales und

[26] *Rat für nachhaltige Entwicklung (Hrsg.)*, Nachhaltige Entwicklung.
[27] Vgl. *Elkington (Hrsg.)*, Cannibals with forks: The triple bottom line of 21st century business.
[28] Vgl. *Weber/Georg/Janke/Mack*, Nachhaltigkeit und Controlling, S. 17.
[29] *Sherwood/Pollard*, Responsible Investing – An Introduction to Environmental, Social and Governance Investment, S. 3.

Governance gerecht werden. Dies bedeutet, dass Risiken, die das Unternehmen in den drei Dimensionen birgt, bewertet werden.

Historisch finden diese ihren Ursprung in der Social Responsibly Investing Bewegung in den Jahren 1980 und 1990[30], die unter anderem durch den Vietnamkrieg, die Diskriminierung von Afroamerikanern und die Ungleichbehandlung der Frauen initiiert wurde.[31] Mit der Einberufung von der Global Compact Initiative ("GCI") durch den UN-Generalsekretär, die die Verpflichtung von CEOs enthielt, universelle Nachhaltigkeitsprinzipien und Maßnahmen zur Erreichung der UN-Ziele umzusetzen, sowie der Veröffentlichung des „Who Cares Wins"-Berichts fiel erstmalig der Begriff ESG und damit schlug auch dessen Geburtsstunde.[32] In gemeinsamer Zusammenarbeit griffen die UN Environmental Programme Financial Initiative und Freshfields Bruckhaus Deringer erstmalig die drei ESG-Kriterien im Investmentfokus auf und unterstrichen die Relevanz für Investmentanalysen, um die künftige Leistung eines Unternehmens zu prognostizieren.[33] Alsbald wurden nachhaltige Investitionsentscheidungen von Verbrauchern sowie Anlegern auf Grundlage der drei Kriterien unternommen.[34] Fokus der drei Säulen ist dabei stets der Grundgedanke der Nachhaltigkeit.

2.1.2.1 Environmental

Die Säule **Environmental** inkludiert jene Aspekte, die ein Risiko für die Umwelt oder für das Klima bergen und bietet damit eine Möglichkeit zur Messung des Beitrags eines Unternehmens zum natürlichen Ökosystem. Für Investoren ist in dieser Dimension wichtig, inwiefern das Unternehmen ressourcenschonend produziert. Folglich werden in diesem Kontext die Emissionen, das effiziente Nutzen von Ressourcen innerhalb der Wertschöpfung, die Verschmutzung und Verschwendung sowie die Umweltfreundlichkeit der Produkte des Unternehmens betrachtet.[35] Darunter fallen bspw. Treibhausgasemissionen, Biodiversität, Klimawandel, Luft- und Wasserverschmutzung, Energieeffizienz oder Abholzung der Wälder.[36] Ein Negativbeispiel ist der populäre Abgasskandal von Volkswagen. Dieser sorgte dafür, dass Volkswagen innerhalb weniger Tage vom nachhaltigsten Automobilhersteller von der Ratingagentur RobecoSam herabgestuft und gar vom Rating ausgeschlossen wurde.[37]

2.1.2.2 Social

Unter **Social** werden alle Kriterien subsumiert, die die Beziehung des Unternehmens zu seinen Stakeholdern wie etwa der Gesellschaft, Arbeitnehmern und Kunden betreffen.[38] Es ist daher relevant, wie sich der Verantwortliche für die Zufriedenheit der Mitarbeiter einsetzt und welche Arbeitsatmosphäre und -bedingungen herrschen.[39] Ferner evaluieren Investoren, ob die Institution unter Einhaltung der Geschäftsethiken operiert und vor allem ob die Menschenrechte eingehalten werden.[40] Mitunter umfasst dies auch den Fokus auf

[30] Vgl.*Bailard (Hrsg.),* From SRI to ESG: The Origins of Socially Responsible and Sustainable Investment.
[31] Vgl. *Morningstar (Hrsg.)*, ESG investing Comes of Age.
[32] Vgl. *Financial Sector Initiative (Hrsg.)*, Who Cares Wins, S. 7.
[33] Vgl. *United Nations Environment Programme Finance Initiative (Hrsg.)*, A Legal Framework for the Integration of Environmental, Social and Governance Issues into Institutional Investment.
[34] Vgl. *United Nations Environment Programme Finance Initiative (Hrsg.)*, A Legal Framework for the Integration of Environmental, Social and Governance Issues into Institutional Investment.
[35] Vgl. *Matos*, ESG and Responsible Institutional Investing Around the World, S. 7.
[36] Vgl. *CFA Institute (Hrsg.)*, Environmental, Social, and Governance Issues In Investing, S. 4.
[37] Vgl.*Schmidbauer/Willmroth*, Öko-Fonds schmeißen Volkswagen raus.
[38] Vgl. *Matos*, ESG and Responsible Institutional Investing Around the World, S. 6.
[39] Vgl. *CFA Institute (Hrsg.)*, Environmental, Social, and Governance Issues In Investing, S. 4.
[40] Vgl.*CFA Institute (Hrsg.)*, Environmental, Social, and Governance Issues In Investing, S. 4.

die Integrität der Geschäftstätigkeit sowie die *Datensicherheit*.[41] Überdies werden auch Kriterien wie bspw. die Geschlechtergleichheit und Diversität, die Beziehung zur Gemeinschaft sowie die Einhaltung der Nachhaltigkeitsanforderungen innerhalb der Lieferkette umfasst.[42] Doch auch die Produktsicherheit kann in diesem Kontext im Interesse der Investoren liegen. Jene Aspekte manifestieren sich u.a. in den OECD-Leitsätzen für multinationale Unternehmen, den ILO-Kernarbeitsnormen, den zehn Prinzipien des UN Global Compact sowie in der ISO 26000[43].

2.1.2.3 Governance

Governance definiert den rechtlichen und faktischen Ordnungsrahmen für die Leitung und Überwachung eines Unternehmens, wofür auch der Begriff „Corporate Governance" verwendet wird. Ein Unternehmen muss demnach im Interesse der Anteilseigner agieren, um die Wirtschaftlichkeit und Handlungsfähigkeit des Unternehmens zu gewährleisten.[44] Maßgeblich sind dabei die Maßnahmen der Unternehmensleitung zum Schutz vor feindlichen Übernahmen, die Gleichberechtigung der Stakeholder und inwiefern das Unternehmen fähig ist, die ESG-Paradigmen in die Geschäftstätigkeit und in die Strategie zu integrieren.[45] Dem liegen weiterhin Faktoren wie etwa die Vorstandsvergütung, Struktur des Aufsichtsrates, Whistleblower-Hotline und die Bekämpfung von Bestechung und Korruption zugrunde.[46]

2.1.2.4 Abgrenzung zu Corporate Social Responsibility

In der Tat weist ESG eine Schnittmenge zu Corporate Social Responsibility (im Folgenden „CSR") auf, wodurch die beiden Begriffe häufig gleichbedeutend verwendet werden. Die Europäische Kommission versteht unter CSR die Integration von gesellschaftlichen, ökologischen und ethischen Aspekten sowie Fragen der Menschenrechte in die Geschäftstätigkeit und Geschäftsstrategie eines Unternehmens – unter Berücksichtigung der Anforderungen der Stakeholder.[47] Dabei beruht CSR ebenfalls auf dem The-Triple-Bottom-Line-Ansatz (siehe Abbildung 3), nach dem Unternehmen die drei Ziele Ökologie, Soziales und Ökonomie verfolgen und dadurch einen Mehrwert für alle Akteure generieren sollen.[48] CSR richtet seinen Fokus somit auf die unternehmerische Etablierung der drei Dimensionen im Lichte der Nachhaltigkeit. Es ist demnach festzuhalten, dass sowohl CSR als auch ESG grundsätzlich dieselben Prinzipien pflegen und damit auch dieselben Ziele verfolgen. Jedoch nutzen beide unterschiedliche Ansätze hierzu; während CSR eher auf die intrinsische Motivation der Unternehmen abstellt, geht ESG den Weg über die Investoren – also die der extrinsischen Motivation – und evaluiert mitunter die Einhaltung und Umsetzung der CSR-Dimensionen. Daher werden die Begriffe in dem Kontext im Folgenden nicht synonym verwendet.

---

[41] Vgl. *Deutsche Bank (Hrsg.),* Was ist ESG-Investing?.
[42] Vgl. *CFA Institute (Hrsg.)*, Environmental, Social, and Governance Issues In Investing, S. 4.
[43] Vgl. *Wirtschaftskammer Tirol (Hrsg.)*, Nachhaltige Werte im Unternehmen? Wozu? – Strategiearbeit als Erfolsfaktor.
[44] Vgl. *Regierungskommission (Hrsg.)*, Deutscher Corporate Governance Kodex, S. 2.
[45] Vgl. *CFA Institute (Hrsg.)*, Environmental, Social, and Governance Issues In Investing, S. 4.
[46] Vgl. *CFA Institute (Hrsg.)*, Environmental, Social, and Governance Issues In Investing, S. 4.
[47] Vgl. *Europäische Kommission (Hrsg.)*, Mitteilung der Kommission an das Europäischen Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss und der Regionen. Eine neue EU-Strategie (2011-14) für die soziale Verantwortung der Unternehmen (CSR) /* KOM/2011/0681 endgültig */.
[48] Vgl. *Schneider/ Schmidpeter*, Corporate Social Responsibility – Verantwortungsvolle Unternehmensführung in Theorie und Praxis, S. 325.

2.1.3 Rolle der Sustainable Development Goals

Im Zuge des Gipfeltreffens im Jahre 2015 erließen die Vereinten Nationen 17 Ziele für die nachhaltige Entwicklung und nahmen diese auf die Agenda 2030, der zugleich als „Weltzukunftsvertrag“ fingiert.[49] Aus diesem Vertrag resultiert die Pflicht für die Staaten, allen Menschen bis zum Jahr 2030 ein Leben in Würde zu sichern. Die Agenda 2030 adressiert dabei fünf wesentliche Kernbotschaften, welche simultan den 17 Zielen als Vision übergeordnet sind. Diese lauten: 1. Die Würde des Menschen im Mittelpunkt, 2. den Planeten schützen, 3. Wohlstand für alle fördern, 4. Frieden fördern und 5. Globale Partnerschaften aufbauen.[50] Die 17 Ziele verfolgen dabei im Wesentlichen die Beendigung von Armut und Hunger sowie die Bekämpfung von Ungleichheiten, Stärkung der Selbstbestimmung der Menschen, Geschlechtergerechtigkeit und Sicherung eines guten und vitalen Lebens für alle. Daneben stehen die Förderung des Wohlstandes für alle und die nachhaltige Gestaltung der weltweiten Lebensweisen im Fokus. Außerdem zählen das Respektieren der ökologischen Grenzen, **die Wahrung der Menschrechte – Frieden, gute Regierungsführung und Zugang zur Justiz** sowie der Aufbau globaler Partnerschaften zu einer der UN-Ziele.[51]

Zusammen mit den ESG-Dimensionen bietet sich somit ein Leitfaden zur Umsetzung der Sustainable Development Goals an, der eine Kategorisierung der Ziele in die ESG-Dimensionen vorangestellt werden muss und in Abbildung 3 wiederzufinden ist[52]:

Abbildung 3: Kategorisierung der 17 UN-Ziele in die ESG-Dimensionen.

GeSI (Hrsg.), Digital with Purpose: Delivering a SMARTer2030, online abrufbar unter: https://digitalwithpurpose.gesi.org, zuletzt besucht am 28.09.2022.

[49] Vgl. *United Nations (Hrsg.)*, Do you know all 17 SDGs?.
[50] Vgl. *United Nations (Hrsg.)*, Do you know all 17 SDGs?.
[51] Vgl. *United Nations (Hrsg.)*, Do you know all 17 SDGs?.
[52] Vgl. *GeSI (Hrsg.)*, Digital with Purpose: Delivering a SMARTer2030.

2.1.4 Definition Corporate Digital Responsibility

Corporate Digital Responsibility (im Folgenden „CDR“) ist ein Ausfluss der verantwortungsvollen Unternehmensführung (Corporate Responsibility), die den (freiwilligen) Beitrag der Wirtschaft zu einer nachhaltigen Entwicklung beschreibt, mit dem erweiterten Blickwinkel auf die *digitale* Unternehmensverantwortung.[53] Der Begriff CDR leitet sich in seiner Wortbildung von Corporate (Social) Responsibility ab und wird seit 2016 verwendet.[54] Unter CDR ist grundsätzlich eine freiwillige Selbstverpflichtung von Unternehmen zu verstehen. Sie findet zwar ihren Ursprung in der „Erfüllung gesetzlicher Anforderungen und diverser Standards, die u.a. den Umgang mit personenbezogenen Daten statuieren, jedoch geht diese Selbstverpflichtung über solche Regularien hinaus und umfasst auch weitergehende ethische Überlegungen sowie die grundlegenden Werte, nach denen ein Unternehmen zu arbeiten hat“.[55] Dieser Definition zufolge ist CDR ein fester Bestandteil einer umfassenden Unternehmensverantwortung in einer zunehmenden digitalisierten Wirtschaft und Gesellschaft.[56] Darunter fallen daher „freiwillige unternehmerische Aktivitäten im digitalen Bereich, die über das gesetzliche Vorgeschriebene hinausgehen und die digitale Welt aktiv zum Vorteil der Gesellschaft mitgestalten“.[57] CDR behandelt einerseits den Einsatz der digitalen Nachhaltigkeit wie etwa die Nachhaltigkeit von Daten und Algorithmen[58] und andererseits die Beachtung der sozialen, ökonomischen und ökologischen Effekte digitalen Unternehmenshandelns in der Welt.[59] Die Unternehmensberatung Accenture unterteilt dabei fünf Anwendungsbereiche: Verantwortungsvoller Umgang mit Daten durch Datenschutz und Datensicherheit (digital stewardship), Transparenz über die Nutzung von Kundendaten (digital transparency), Unterstützung von Kunden durch Nudging (digital empowerment), faire Verteilung der Gewinne aus der Nutzung von Kundendaten (digital equity) und die Bereitstellung von Datensätzen für Forschungszwecke (digital inclusion).[60]

2.2 Etablierung des Datenschutzes in der ESG-Dimension

2.2.1 Datenschutz: Die Achillesferse der Digitalisierung?

Der exponentielle Anstieg der Digitalisierung[61] verursacht ambivalente Auswirkungen und bedingt auch in diesem Kontext ein Umdenken im unternehmerischen Handeln, das über das gesetzlich Geforderte hinaus geht. Eine zunehmende Digitalisierung wirft Fragen in vielerlei Hinsichten auf. So sind Konsequenzen z.B. durch den digitalen Machtmissbrauch und die Überwachung, ob staatlich oder wirtschaftsgetrieben, Freiheitseinschränkungen durch persönliches Scoring, Profiling oder andere Formen der Netzmanipulation in Erwägung zu ziehen.[62] Die Daten der Kunden, Beschäftigten usw. werden zu zentralen Gütern, welche der Kommerzialisierung unterworfen werden. Diese Daten stellen dabei eine maßgebliche Grundlage für die unternehmerische Wertschöpfung dar und tragen einen

[53] Vgl. u.a. *Herden/Alliu/Cormier*, Corporate Digital Responsibility, S. 17.
[54] Vgl. *Cooper/Siu/Wei*, Corporate digital responsibility- Doing well by doing good; *Dörr*, Praxisleitfaden Corporate Digital Responsibility, S. 38.
[55] *Global Intelligence for the CIO (Hrsg.)*, The rise of corporate digital responsibility.
[56] Vgl. *Dörr*, Praxisleitfaden Corporate Digital Responsibility, S. 35.
[57] *Bundesministerium der Justiz und Verbraucherschutz (Hrsg.)*, Corporate Digital Responsibility: Digitalisierung verantwortungsvoll gestalten, S. 1.
[58] Vgl. u.a. Smart-Data-Begleitforschung (Hrsg.), Corporate Digital Responsibility, S. 8 f.
[59] Vgl. *Esselmann/Golle/Thiel/Brink*, Corporate Digital Responsibility – Unternehmerische Verantwortung als Chance für die deutsche Wirtschaft.
[60] Vgl. *Cooper/Siu/Wei*, Corporate digital responsibility – Doing well by doing good, S. 2 f.
[61] Vgl. *Dörr*, Praxisleitfaden Corporate Digital Responsibility, S. 9 ff.
[62] *Dörr*, Praxisleitfaden Corporate Digital Responsibility, S. 35.

wesentlichen Beitrag u.a. zum Marketing oder zur Produktentwicklung bei.[63] Vor diesem Hintergrund bewegt sich der Datenschutz immer mehr ins Bewusstsein der Menschen, wie die Studie von Deloitte aufzeigt. Zwar ist den Konsumenten der digitale Mehrwert bspw. von Smart Home bewusster im Vergleich zur Umfrage von 2015, allerdings lässt sich in der neuen Studie auch eine Zunahme an Bedenken am Datenschutz verzeichnen; damit wird der mangelnde Datenschutz auf Platz zwei als Grund für die Nichtnutzung von Smart Home-Produkten rangiert.[64] Diese Tatsachen postulieren, der Digitalisierung die neue Verantwortung aufzubürden, die Persönlichkeitsrechte jedes einzelnen Individuums zu beachten.[65] Auch die Covid-19-Pandemie erwies sich in den letzten zwei Jahren als starker Treiber der Digitalisierung und damit der Relevanz des Datenschutzes. Als Maßnahmen zur Minderung des Infektionsrisikos wurden unter anderem Beschäftigten von Unternehmen eine Homeoffice-Pflicht verordnet, aber auch der Einsatz von Corona-Apps ließen das Bewusstsein der Bürger und Bürgerinnen in einer noch nie dagewesenen Geschwindigkeit steigen. Dieses dynamische Umfeld stellt Unternehmen vor diversen Herausforderungen bei der Umsetzung der Datenschutzvorschriften.[66] Da Gesetze bei der rapiden Zunahme an digitalen Anwendungen schnell an ihre Grenzen stoßen, ist es jedoch unerlässlich, dass der Datenschutz zusätzlich durch Investoren und Anleger getrieben wird und ein weiterer Anreiz für die Unternehmen zum nachhaltigen Umgang mit personenbezogenen Daten entsteht.

2.2.2 Corporate Digital Responsibility: Datenschutz als Nachhaltigkeitsverpflichtung

Ein Ansatz ist, dass der Datenschutz als eine Nachhaltigkeitsverpflichtung den Unternehmen auferlegt wird, die aus einer Corporate Digital Responsibility herauswächst. Daraufhin wird eine Etablierung des Datenschutzes in die ESG-Dimension angestrebt, mit dem Ziel, zusätzlich einen (monetären) Anreiz für Unternehmen zur Umsetzung des Datenschutzes zu schaffen (Pull-Methode), indem hierdurch der Shareholdervalue maximiert wird. Fraglich ist demnach, ob sich für Unternehmen eine digitale Verantwortung in Form der nachhaltigen Datenverarbeitung[67] gegenüber der Gesellschaft und Umwelt ergibt.[68] Damit der Datenschutz als Nachhaltigkeitsverpflichtung und damit als ESG-Anliegen verstanden wird, muss dieser Auswirkungen auf die Allgemeinheit und auf künftige Generationen haben. Dabei sind die Folgen eines nichtkonformen Umganges mit personenbezogenen Daten keineswegs nur auf ein Individuum beschränkt, sondern können eklatante Auswirkungen auf das Gemeinwohl und gar für künftige Generationen haben – was der Datenskandal von Cambridge Analytica verdeutlicht.[69] Das Datenanalyseunternehmen erstellte psychologische Profile von über 87 Millionen Facebook-Nutzern und nutzte hier-

[63] Vgl. *Dörr*, Praxisleitfaden Corporate Digital Responsibility, S. 35.
[64] Vgl. *Deloitte (Hrsg.)*, Smart Home Consumer Survey 2018 – Ausgewählte Ergebnisse für den deutschen Markt, S. 13.
[65] Vgl. *Dörr*, Praxisleitfaden Corporate Digital Responsibility, S. 35.
[66] Vgl. die starke Zunahme an Praxishilfen zur Handhabung des Datenschutzes in der Covid-19-Pandemie: u.a. *GDD (Hrsg.)*, Datenschutz und Corona; *Datenschutz.org (Hrsg.)*, Datenschutz während der Corona-Pandemie: Was ist erlaubt, was nicht?.
[67] „Verarbeitung" i.S.d. Art. 4 Nr. 2 DSGVO: „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
[68] Vgl. *Basecamp (Hrsg.)*, Nachhaltigkeit und Datenschutz: Neues von der CDR-Initiative.
[69] Vgl. *New York Times (Hrsg.),* Cambridge Analytica and Facebook: The Scandal and the Fallout So Far.

für persönliche Daten von über 200.000 Facebook-Nutzern. Cambridge Analytica erhob im Rahmen einer freiwilligen Umfrage Daten von 200.000 Nutzern, die jedoch nicht über die Nutzung ihrer persönlichen Daten informiert wurden. Auch die weiteren 87 Millionen Nutzer waren in Unkenntnis über die von ihnen erstellten Profile.[70] Dies ermöglichte es diversen Politikern auf Grundlage dieser Daten und Informationen, ihre Werbemaßnahmen auf die Profile und Präferenzen der Nutzer zuzuschneiden. Auf diesem Wege nahmen Parteien und Politiker Einfluss auf die Wähler sowie deren Wahlentscheidungen und manipulierten so die Wahlen. Es ist daher unumstritten, dass sich das Ausnutzen personenbezogener Daten auch auf die Wahlentscheidung und damit die neue Besetzung der Regierung und sogar auf den grundlegendsten Wert der Demokratie auswirkt.[71] Personenbezogene Daten eröffnen also nicht nur den Weg zu vulnerablen Erkenntnissen der betroffenen Person selbst und zur Beeinflussung dieser, sondern können bei einer bestimmten Menge an vorhandenen Daten die Zusammensetzung einer Regierung und damit die Zukunft einer gesamten Gesellschaft dirigieren. Zudem spielt die Datenverarbeitung von Verbrauchern auch im Kontext der freien Wirtschaft eine immens große Rolle. Big Data ermöglicht es Unternehmen zudem, ihre Kunden durch eine Unmenge an Informationen und Daten zu analysieren, um daraufhin ihr/e Produktangebot oder Marketingmaßnahmen auf den einzelnen Kunden individuell anzupassen. Darunter fallen auch sensible Informationen, die den Kunden besonders vulnerabel machen. Dieser Umstand postuliert nicht nur einen regulären Schutz der Betroffenen, sondern dass Unternehmen moralische und ethische Prinzipien bei der Verarbeitung dieser Daten wahren. Nur durch einen gewissenhaften und nachhaltigen Umgang mit Daten kann sichergestellt werden, dass Daten der betroffenen Personen nicht zweckentfremdet oder ausgenutzt werden. Datenschutz kann jedoch auch eine ökologische Nachhaltigkeitskomponente aufweisen und kann aufgrund des Grundsatzes der Datenminimierung redundanter Speicherung von Daten entgegenwirken und folglich den Energieverbrauch von Rechenzentren minimieren.[72] Schlussfolgernd sollten Unternehmen nicht nur aufgrund von Regularien und extrinsischer Forcierung den Datenschutz achten, sondern auch um nachhaltige Digitalisierung im Rahmen der CDR zum Wohle der gesamten Gesellschaft zu ermöglichen. Es ist also davon auszugehen, dass der Schutz personenbezogener Daten in Anbetracht der Risiken für die Betroffenen eine Nachhaltigkeitsverpflichtung für alle Akteure darstellt.

2.3 Verortung des Datenschutzes in den ESG-Dimensionen

Ferner ist strittig, wo der Datenschutz in der gesamten ESG-Ära angesiedelt wird, da dem Datenschutz Elemente aus allen drei ESG-Säulen innewohnen.[73] Es bleibt somit zu klären, in welchen der drei ESG-Dimensionen der Datenschutz mit Hinblick auf den Schutzzweck und Historie verortet werden kann. Daher ist es unabdingbar, den Ursprung sowie Zweck und Ziele des Datenschutzes zu analysieren, um daraufhin einen Konsens zu finden.

2.3.1 Analyse des Begriffes des Datenschutzes

Zuallererst ist somit die Historie des Datenschutzes zu beleuchten und anschließend der Schutzzweck vor dem ESG-Hintergrund zu untersuchen. Eine konkrete Definition für den

[70] Vgl. *Heawood*, Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal, S. 429.
[71] Vgl. *Heawood*, Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal, S. 431 f.
[72] Vgl.*PWC (Hrsg.)*, Unterstützt Ihr Datenschutzprogramm Ihre ESG-Bemühungen?.
[73] Vgl. *Redclover Advisors (Hrsg.)*, Data Privacy & ESG.

Datenschutz existiert nicht, jedoch kann darunter primär der Schutz personenbezogener Daten vor missbräuchlicher Verwendung und Datenverarbeitung verstanden werden, um das Recht des Einzelnen auf informationelle Selbstbestimmung zu stärken.[74]

2.3.1.1 Historie und Entstehung des Datenschutzes

Erste Diskussionen zum Datenschutz fanden in den USA bereits in den Sechzigern statt, allerdings wurde das erste Gesetz zum Datenschutz ca. zehn Jahre später im Jahre 1970 im deutschen Hessen erlassen. Damit ebnete Deutschland als erster Staat den Weg für die Etablierung des Datenschutzes in die Rechtspraktik, auch wenn die praktische Anwendung dessen aufgrund mangelnder digitaler und elektronischer Datenverarbeitungsvorgänge von niedriger Bedeutung war. Vor dem Hintergrund einer bundesweiten Harmonisierung erließ der deutsche Gesetzgeber im Jahr 1977 daraufhin das erste Bundesdatenschutzgesetz.[75] Die öffentliche Wahrnehmung nahm jedoch mit dem „Volkszählungsurteil“[76], welches vom Bundesverfassungsgericht am 15.12.1983 beschlossen wurde, rapide zu. Da die Tragweite und die Auswirkungen jenes Urteils bis ins Gegenwärtige reichen, gilt dieses auch als „die Geburtsstunde des Datenschutzes“.[77] Im Hinblick auf die Definitionen von ESG und die der Nachhaltigkeit sind jedoch der folgende Gegenstand und der Hintergrund des Volkszählungsurteils erheblich: Dem Urteil lag der Plan des deutschen Gesetzgebers zugrunde, eine umfassende Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung durchzuführen. Allerdings waren neben der bloßen Volkszählung auch private Informationen wie etwa Angaben über Religionszugehörigkeit sowie über die finanzielle Lage anzugeben; diese Umstände führten zu einem öffentlichen Widerstand. Wegweisend kam das Bundesverfassungsgericht dem Widerstand nach und begründete in diesem Präzedenzfall das Recht auf informationelle Selbstbestimmung als geschütztes Rechtsgut i.S.d. Verfassungsrechts. Folgerichtig erkannte das Bundesverfassungsrecht bereits zu jener Zeit an, dass die stetig zunehmende Digitalisierung eine erhöhte Schutzbedürftigkeit der betroffenen Person(en)[78] erfordert und das Interesse der Betroffenen am Schutz ihrer personenbezogenen Daten bedingt.[79] Jenes Urteil stellte damit den Meilenstein in der Geschichte der datenschutzrechtlichen Gesetzgebung dar und hatte eine ausschlaggebende Wirkung für die Novellierung des Bundesdatenschutzgesetztes im Jahre 1995. Seither gilt der Datenschutz als festes Element des Grundgesetzes und leistet einen maßgeblichen Beitrag zum Verständnis von datenschutzrechtlichen Regelwerken, aber auch für die Assoziation zur Nachhaltigkeit im Umgang mit Daten: dem Widerstand der Bürger gegen eine extensive Erhebung von Daten durch den Staat und einer hierauf ergangenen Entscheidung des Bundesverfassungsgerichts, welches jedem einzelnen Bürger ein Recht auf informationelle Selbstbestimmung einräumt.[80]

---

[74] Vgl. *Schröder*, Datenschutzrecht für die Praxis, 2. Kapitel Punkt I 1.
[75] Vgl. *Schröder*, in: Datenschutzrecht für die Praxis, 1. Kapitel Punkt I 1.
[76] Vgl. BVerfG, Urteil des Ersten Senats vom 15.12.1983, NJW 1307, 1307 ff.
[77] Vgl. *Schröder*, in: Datenschutzrecht für die Praxis, 1. Kapitel Punkt I 1.
[78] „Betroffene Person“ i.S.d. Art. 4 Nr. 1 DSGVO: „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
[79] Vgl. BVerfG, Urteil des Ersten Senats vom 15.12.1983, NJW 1307, 1307 ff.
[80] Vgl. *Schröder*, Datenschutzrecht für die Praxis, 1. Kapitel Punkt I 1.

2.3.1.2 Analyse des Schutzzwecks der DSGVO

Im Lichte einer gerechten Einordnung des Datenschutzes in eine der drei ESG-Dimensionen ist von Bedeutung, was der Gegenstand und Schutzzweck des Datenschutzes sind. Ziel und Gegenstand der DSGVO sind gem. Art. 1 Abs. 1 DSGVO der Schutz der natürlichen Personen bei der Verarbeitung ihrer personenbezogenen Daten und die Gewährleistung des freien Verkehrs dieser Daten. Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine leichte Tendenz zur Einordnung in der Social-Säule lässt sich aufgrund des Umstandes abbilden, dass der Schutz der personenbezogenen Daten in Art. 8 Abs. 1 der Charta der Europäischen Grundrechte[81] verankert und damit ein Grundrecht ist. Nicht unerheblich ist dabei die Tatsache, dass es sich um ein ausdrücklich normiertes Menschenrecht ungeachtet der Staatsangehörigkeit oder des Aufenthaltsortes der Person handelt (ErwGr. 14). Parallel zu dem sind nach Ansicht der EuGH auch weitere Grundrechte betroffen.[82] Daneben kann die Verarbeitung von personenbezogenen Daten auch mittelbar Implikationen für die Freiheit der Meinungsäußerung haben.[83] Bereits im Volkszählungsurteil erkannte das Bundesverfassungsgericht die Folgen der Datenverarbeitung auf weitere Grundrechte an, die elementar für die Aufrechterhaltung und das Funktionieren eines demokratischen Staates sind, wie etwa auf die Versammlungs- und Vereinigungsfreiheit.[84] Darüber hinaus gewinnt der Schutz vor Diskriminierung nach Art. 21 Abs. 1 GRC mit Hinblick auf die zunehmenden automatisierten Einzelentscheidungsfindungen sukzessive an Bedeutung. Jene Entscheidungen beruhen i.d.R. auf der Verarbeitung besonderer Kategorien personenbezogener Daten unter Zuhilfenahme von Algorithmen und künstlicher Intelligenz, welche (auch unbeabsichtigt) diskriminierende Elemente beinhalten und für die betroffene Person erhebliche Konsequenzen haben können (ErwGr. 71, S. 2). Zu betonen ist dabei, dass ErwGr. 2, S. 2 explizit erwähnt, dass die „DSGVO zur Vollendung eines Raumes der Freiheit, der Sicherheit und des Rechtes und einer Wirtschaftsunion, zum wirtschaftlichen und **sozialen Fortschritt**, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarktes sowie zum **Wohlergehen der Menschen** beitragen soll“.

2.3.2 Zwischenfazit

Es bleibt also festzuhalten, dass der Datenschutz von dem Menschenrechtsgedanken dominiert wird und dieser die Triebfeder der DSGVO ist. Dabei ist es unerheblich, dass sich aus den Normen der DSGVO gesetzliche Verpflichtungen für die Verantwortlichen[85] ergeben und auch mit empfindlichen Sanktionen einhergehen. Bei diesen handelt es sich lediglich um Konsequenzen bei einer Nichtumsetzung durch die Verantwortlichen und nicht um den Kernbestandteil der DSGVO und des Rechts auf informationelle Selbstbestimmung. Zwar ist datenschutzkonforme Wertschöpfung auch Teil der guten Unternehmensführung und einer Compliance-Kultur, jedoch sind dies die Ausflüsse der sich aus

---

[81] Vgl. *Amtsblatt der Europäischen Union (Hrsg.)*, Charta der Grundrechte der Europäischen Union – (2010/C 83/02).

[82] Vgl. EuGH, Urteil vom 13.5.2014 - C-131/12, ZD 2014, 356, 361.

[83] Vgl. EuGH (Große Kammer), Urteil vom 21.12.2016 – C-203/15, C-698/15, EuZW 2017, 153, 160.

[84] Vgl. BVerfG, Urteil des Ersten Senats vom 15.12.1983, NJW 1307, 1307 ff.

[85] „Verantwortlicher“ i.S.d. Art. 4 Nr. 7 DSGVO: „Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.“

der DSGVO ergebenden Anforderungen und keine freiwilligen Selbstverpflichtungen. Selbiges gilt auch für die Einordnung in die Environment-Dimension; zwar mögen sich aus gewissen Grundsätzen der DSGVO wie etwa der Datenminimierung latente positive Auswirkungen auf die Umwelt ergeben, indem weniger Speicherkapazitäten beansprucht werden und die Energieeffizienz erhöht wird, allerdings handelte es sich um eine weite Auslegung dieses Grundsatzes, die nicht im Kerngedanken des Datenschutzes verankert ist.[86] Die Tatsache jedoch, dass die DSGVO nach ErwGr. 2, S. 2 daneben den sozialen Fortschritt und das Gemeinwohl fördern soll, macht deutlich, dass sich die Verfolgung eines angemessenen Datenschutzes zugunsten einer gesamten Gesellschaft auswirkt und auch die Beziehungen des Verantwortlichen zu den Stakeholdern nachhaltig stärkt. Damit stimmen diese Werte und Prinzipien mit denen der sozialen Säule überein, die insbesondere auf die Einhaltung der Menschenrechte abzielt. In Anbetracht dieser Parallelen zwischen den Zielen des Datenschutzes und der Social-Dimension ist es naheliegend, nachhaltigen Umgang mit Daten und damit den Datenschutz als integralen Bestandteil der Social-Komponente anzusehen.

2.4 Spannungsfeld innerhalb von ESG durch Korrelationen mit dem Datenschutz

Ambitionen der einzelnen Dimensionen geraten oftmals in ein Kollisionsdilemma, welches in Zielkonflikte resultiert. So wurden bspw. Konfliktpotenziale bei der Umsetzung ökologischer Maßnahmen identifiziert, die die wirtschaftliche Situation finanziell schwacher Menschen gefährden kann und damit eine Kollision zur Social-Komponente entstehen lässt.[87] Dieses Dilemma sucht seinesgleichen in der Beziehung der ESG-Säulen zu dem Datenschutz. Dabei können die Kollisionen facettenreich sein und in vielerlei Formen auftreten. Jedoch lassen sich solche Kollisionen nicht nur im Verhältnis zwischen den einzelnen Säulen erkennen, vielmehr können auch Maßnahmen derselben Säule in Konflikte geraten. So können Unternehmungen der Social-Säule ebenso im Widerspruch zum Datenschutz stehen wie säulenübergreifend mit der E- und G-Dimension. Mit der Verarbeitung von personenbezogenen Daten gehen Pflichten aus der DSGVO einher, die durch die Verantwortlichen zu erfüllen sind. Bei einem Verstoß dieser Pflichten drohen zum einen nach Art. 83 DSGVO empfindliche Bußgelder bis zu vier Prozent des weltweiten erzielten Jahresumsatzes. Zum anderen stehen betroffenen Personen, denen aufgrund eines Verstoßes ein materieller oder immaterieller Schaden entstanden ist, dezidierte Schadensersatzansprüche zu (Art. 82 DSGVO). Risikominimierende Maßnahmen der ESG-Säulen, welche nicht im Einklang mit dem Datenschutz stehen, erscheinen somit in dieser Hinsicht kontraproduktiv und erhöhen demzufolge das Risiko eines Verstoßes gegen die DSGVO und damit eines Bußgeldes. Ein solches Bußgeld kann darüber hinaus eine Kettenreaktion auslösen und unmittelbar das Risiko in anderen ESG-Säulen erhöhen. Folglich findet eine Risikoverlagerung statt, was nicht im Sinne der ESG- Dimension stehen sollte. Dadurch entstehen innerhalb der Paradigmen Korrelationen und ein Ungleichgewicht, die ein Spannungsverhältnis in der ESG-Ära verursachen, welches es auszugleichen gilt. Es sind daher Prozesse und Strategien zu definieren, die alle drei Dimensionen in Einklang mit dem Datenschutz bringen. Nachfolgend wird anhand von Beispielen die Ambivalenz zwischen und innerhalb der Dimensionen verdeutlicht und auch Strategien zur Schaffung

[86] Vgl. *Redclover Advisors (Hrsg.)*, Data Privacy & ESG.
[87] Vgl. *Umweltbundesamt (Hrsg.)*, Soziale Aspekte des Umweltschutzes/Ökologische Gerechtigkeit.

einer Balance aufgezeigt, sodass der Datenschutz vielmehr als Teil der Lösung sowie Förderer der Digitalisierung anzusehen ist.

2.4.1 Zielkonflikte zwischen Environment und Datenschutz am Beispiel von Hybrid-Fahrzeugen mit automatisiertem Fahrbetrieb und kohärentem Bonussystem

Im Zuge der Senkung der CO2-Steuer werden im Environmental Paradigma vermehrt Hybrid-Fahrzeuge eingesetzt, welche mittels Geofencedaten automatisiert in den elektrischen Fahrbetrieb schalten, sobald vordefinierte Grenzen überschritten werden. So senken Automobilhersteller ihren CO2-Ausstoß und damit auch die Höhe der abzugebenden CO2-Steuer. BMW hat im vergangenen Jahr ein Bonus-Punktesystem für elektrisches Fahren mit Plug-In-Hybrid (im Folgenden „PHEV“) eingeführt, das hohe elektrische Fahranteile durch die Vergabe von Bonuspunkten belohnt. In den eDrive Zones werden zwei BMW Points pro elektrisch gefahrenem Kilometer angerechnet, außerhalb der eDrive Zones ist es ein BMW Point pro Kilometer. Ähnlich dem Payback-Konzept können die Punkte für die gefahrenen Kilometer gesammelt und bspw. gegen Lade-Guthaben eingelöst werden. Dies ist aber erst ab einer bestimmten Punkteanzahl möglich. Dabei entsprechen 1.250 BMW Points einem Guthaben von 10 Euro. Für 3.000 Punkte werden 25 Euro, für 5.800 Punkte 50 Euro gutgeschrieben. Auf diese Weise können Fahrer eines PHEV-Models der Marke BMW mit jedem rein elektrisch zurückgelegten Kilometer aktiv zur Reduzierung von CO2-Emissionen beitragen und dabei gleichzeitig die Betriebskosten ihres Fahrzeugs senken.[88]

2.4.1.1 Funktionsweise des automatisierten Fahrbetriebes in eDrive Zones

Die Funktionsweise der automatischen Umstellung in den elektrischen Fahrbetrieb beruht auf der Geofencing-Technologie. Darunter versteht man das automatisierte Auslösen einer technischen Funktion (zum Beispiel den Wechsel vom Verbrennungsmotor in den elektrischen Fahrbetrieb) durch das Überschreiten eines geografisch definierten Bereichs (wie etwa beim Einfahren in eine städtische Umweltzone). Demnach handelt es sich dabei um eine Positionierungstechnik, bei der räumliche und zeitliche Aufenthalte anhand der Echtzeit des Fahrzeuges mittels GPS-Daten erfasst werden (siehe Abbildung 4).[89] Derweil bestimmt das GPS die satellitengestützte Position. Daten wie der Aufenthalt innerhalb der Zone und die Begrenzung werden vom Geofencing-System, der fahrzeuginternen Ausstattung oder von beiden gespeichert und verarbeitet. Die definierten Zonen enthalten Verkehrsregeln und Informationen als Attribute, die den Fahrzeugen und Fahrern als intelligenter Verkehrsdienst zur Verfügung gestellt werden.[90] Das Pilotprojekt Geofencing for Smart Urban Mobility (im Folgenden: GeoSUM), das von der Straßenüberwachungsbehörde von Norwegen durchgeführt wurde, illustriert die Vorgehensweise von Geofencing wie folgt: Es werden dezidierte Bereiche in einem Gebiet als Umweltzonen im Vorab definiert (grün gekennzeichnete Low emission zone). Der Fahrer des Fahrzeugs erhält über das Infotainment-System eine Mitteilung, sobald jener sich solch einer vordefinierten Umweltzone nähert. Daraufhin schaltet das Fahrzeug automatisch vom Verbrennungsmotor in den elektrischen Fahrbetrieb.

[88] Vgl. *BMW Group (Hrsg.)*, Elektrisch fahren, BMW Points sammeln, kostenfrei laden: BMW präsentiert weltweit erstes Prämienprogramm für Fahrer von Plug-in-Hybrid-Modellen.
[89] Vgl. *National Acadamies (Hrsg.)*, Geofencing for Smart Urban Mobility: Effects From a Pilot With Retrofit Equipment.
[90] Vgl. *Nait-Sidi-Moh/Bakhouya/Gaber/Wack*, Geopositioning and Mobility, S. 127.

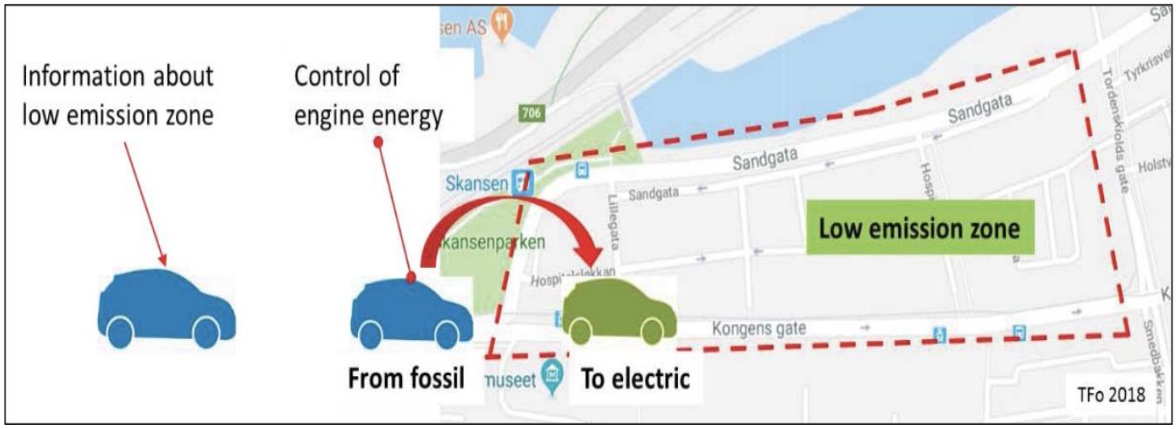

Abbildung 4: Use case 2: Approaching a CZ boundary and Vehicle power is changed to electricity.

Sintef (Hrsg.), Geofencing for Smart Urban Mobility, online abrufbar unter: https://sintef.brage.unit.no/sintef-xmlui/bitstream/handle/11250/2643877/2020-00100_Geofencing%2bfor%2bsmart%2burban%2bmobility.pdf?sequence=2&isAllowed=y, zuletzt besucht am 28.09.2022.

Die Daten über den Aufenthalt, die gefahrenen Kilometer etc. werden sodann an die Hersteller-App wie bspw. an die My BMW App übertragen.[91] Hierzu muss der BMW PHEV mit der BMW ID, die sich aus der E-Mail-Adresse und dem Passwort zusammensetzt, in der My BMW App verbunden sein.[92] Über die App, die auf dem Smartphone des Fahrers installiert wird, kann der Fahrer daraufhin den Punktestand einsehen und verwalten. Hierüber erfolgt auch das Einlösen der BMW Points in Kombination mit dem digitalen Ladeservice BMW Charging.[93]

2.4.1.2 Datenschutzrechtliche Implikationen des Einsatzes von Plug-in-Hybrid-Fahrzeugen mit automatischem Schaltmechanismus

Da beim Einsatz von PHEVs, die automatisch in den elektrischen Fahrbetrieb schalten, der genaue Standort des Fahrers mit Hilfe von GPS-Daten ermittelt wird, sind in diesem Kontext datenschutzrechtliche Implikationen zu untersuchen. Fraglich ist, ob die DSGVO auf die Verarbeitung von GPS-Daten anzuwenden ist und ob diese unter der Definition der personenbezogenen Daten nach Art. 4 Nr. 1 DSGVO fallen. Die Norm erfasst alle Informationen als „personenbezogene Daten“, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu **Standortdaten**, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann, Art. 4 Nr. 1 DSGVO. Da über den Fahrer während der Fahrtzeit Daten wie etwa befahrene Bereiche, der Aufenthalt und die Dauer des Aufenthalts in den befahrenen Bereichen und die Kilometeranzahl verarbeitet, ist der Personenbezug zu bejahen. Der Personenbezug wird insbesondere dadurch hergestellt, dass diese Daten i.d.R. zusammen mit der Fahrzeugidentifikationsnummer verarbeitet werden, um die gefahrenen Kilometer dem Fahrer oder Fahrzeug in der App zuordnen zu können.[94] Damit handelt es sich bei den betreffenden Daten um personenbezogene Daten i.S.d. DSGVO, wodurch der Anwendungsbereich eröffnet ist. Für den

[91] Vgl. *Nait-Sidi-Moh/Bakhouya/Gaber/Wack*, Geopositioning and Mobility, S. 127.
[92] Vgl. *BMW (Hrsg.)*, Fragen und Antworten der BMW Kundenbetreuung.
[93] Vgl. *BMW (Hrsg.)*, Fragen und Antworten der BMW Kundenbetreuung.
[94] Vgl. *BMW (Hrsg.)*, Rechtliche Hinweise zum Datenschutz, S. 27.

Verantwortlichen wachsen somit gem. Art. 2 Abs. 1 DSGVO aus den Vorschriften datenschutzrechtliche Verpflichtungen heraus, die bei der Verarbeitung dieser Daten zu erfüllen sind. Dabei sind aber insbesondere die Folgen aus der Verarbeitung für den Betroffenen in Erwägung zu ziehen.

2.4.1.2.1 Rechtmäßigkeit der Verarbeitung

Für die Rechtmäßigkeit einer Verarbeitung bedarf es einer Rechtsgrundlage aus Art. 6 DSGVO (sog. Verbot mit Erlaubnisvorbehalt). Während die Verarbeitung der Standortdaten im Verhältnis zum Kunden auf eine Einwilligung i.S.d. Art. 88 DSGVO i.V.m. § 26 Bundesdatenschutzgesetz (im Folgenden „BDSG“) gestützt werden kann, erweist sich diese Rechtsgrundlage im Beschäftigungskontext als strittig. Für eine wirksame Einwilligung wird das Kernelement der Freiwilligkeit vorausgesetzt (Art. 7 DSGVO in Verbindung mit ErwGr. 43), die im Verhältnis Arbeitgeber und Arbeitnehmer nicht zweifelsfrei bejaht werden kann. Aufgrund des zwischen den Arbeitgebern und den Beschäftigten existierenden Über-/Unterordnungsverhältnis steht jedoch regelmäßig in Frage, ob Beschäftigte gegenüber ihrem Arbeitgeber tatsächlich freiwillig ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten erteilen können.[95] Die Freiwilligkeit dürfte bereits dann entfallen, wenn sich die betroffene Person im Beschäftigungsverhältnis beeinflusst, gedrängt, bestimmt oder gezwungen sieht, ohne dass es einer Zwangsausübung bedarf.[96] Eine Rechtmäßigkeit auf Grundlage einer Einwilligung wäre in dem Fall dann denkbar, wenn weitere technische Maßnahmen getroffen werden. Unabdingbar wäre es hierbei, dass der Beschäftigte jederzeit die GPS-Ortung ausschalten kann – insbesondere bei privater Nutzung von Dienstfahrzeugen.[97] Allerdings ist die Diskussion hierüber ohnehin hinfällig, da die Effektivität des Einsatzes jener PHEVs in Frage zu stellen ist, wenn der Beschäftigte die Funktion der automatisierten Schaltung in den elektrischen Fahrbetrieb jederzeit ausschalten kann.

In Betracht könnte daher die Verarbeitung dieser Daten auf Grundlage des berechtigten Interesses des Verantwortlichen nach Art. 88 i.V.m. 6 Absatz 1 lit. f DSGVO kommen. Hiernach ist die Verarbeitung dann rechtmäßig, wenn diese zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Es ist also zu eruieren, ob das Interesse des Verantwortlichen an der Verarbeitung der Standortdaten das Interesse der Beschäftigten am Schutz seiner Privatsphäre überwiegt. Die Prüfung des berechtigten Interesses des Verantwortlichen wird in drei Schritten vorgenommen, in denen die drei folgenden Voraussetzungen kumulativ vorliegen müssen: Zunächst muss es sich um ein **berechtigtes Interesse** handeln. Im nächsten Schritt werden die **Interessen und Grundrechte der betroffenen Person** untersucht und anschließend die Erforderlichkeit dieser Verarbeitung geprüft.

Das Interesse des Verantwortlichen an einem erhöhten Umweltschutz sowie Senkung der CO2-Steuer sind überwiegend sozialer sowie betriebswirtschaftlicher Natur und verstoßen weder gegen Gesetze anderer Rechtsordnungen, noch handelt es sich hierbei um eine verbotene Handlung. Folglich dürfte es sich hierbei um ein legitimes Interesse seitens des Verantwortlichen handeln.

---

[95] Vgl. VG Lüneburg, Teilurteil vom 19.3.2019 – 4 A 12/19, ZD 2019, 331 Rn. 62; *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Hrsg.)*, Tätigkeitsbericht 2019, S. 103; *Unabhängiges Datenschutzzentrum Saarland (Hrsg.)*, 27. Tätigkeitsbericht, S. 82.

[96] Vgl. *Datenschutzkonferenz (Hrsg.)*, Kurzpapier Nr. 14: Beschäftigtendatenschutz, S. 1 f.

[97] Vgl. VG Wiesbaden, Urteil vom 17.01.2022 – 6 K 1164/21.WI, ZD 2022, 406, 409.

Mit der Verarbeitung der Standortdaten verfolgt der Verantwortliche zum einen das Interesse, die Treibhausgas-Emissionen zu verringern und folglich den Umweltschutz zu fördern. Das primäre Interesse des Verantwortlichen besteht jedoch vorrangig in der Reduzierung der CO2-Bepreisung, die nach dem Brennstoffemissionshandelsgesetz anfällt. Die Verarbeitung der Standortdaten ermöglicht es, dass das Fahrzeug insbesondere in Zonen, die durch Treibhausgase oder Feinstaub stark belastet sind, automatisiert in den elektrischen Fahrbetrieb schaltet. Hierdurch werden die Dauer und gefahrenen Kilometer reduziert, in dem das Fahrzeug mit dem Verbrennungsmotor betrieben wird. Dies wiederum führt zur Senkung des CO2-Preises. Eine emissionsarme oder gar emissionsfreie Umwelt liegt nicht nur im Interesse der Allgemeinheit, sondern tangiert das Existenzbedürfnis der Menschheit. Naturkatastrophen bedingt durch den Klimawandel riskieren – wie bereits oben beschrieben – auch Existenzen und fundamentale Bedürfnisse wie etwa den Verlust der Ernte für die Landwirtschaft.[98] Hiermit steht es auch im Interesse der Allgemeinheit, emissionsfreie Fahrzeuge einzusetzen, um die ökologische Nachhaltigkeit zu fördern, die der Verantwortliche durch den Einsatz der PHEVs mit der automatisierten Schaltung unterstützt.

Dem Verantwortlichen stehen überdies keine milderen Mittel zur Verfügung. Bisher werden PHEVs primär aufgrund der Steuervorteile erworben oder aufgrund dessen durch Beschäftigte geleast; dies ist auch die Ursache, weshalb der elektrische Fahrbetrieb nur mäßig oder kaum eingesetzt wird.[99] Folglich ist die Datenverarbeitung auch erforderlich. Dem hingegen sind jedoch die Interessen der Beschäftigten abzuwägen. Das Interesse des Beschäftigten bezieht sich auf die Wahrung des Rechts auf informationelle Selbstbestimmung und der Privatsphäre insbesondere gegenüber dem Arbeitgeber. Von Bedeutung ist dabei, dass Beschäftigte keiner Leistungskontrolle ausgesetzt sein dürfen. Der Verantwortliche erlangt hierdurch die Möglichkeit, die Fahrten der Arbeitnehmer zu überwachen und dabei Rückschlüsse auf den Aufenthalt während oder gar außerhalb der Arbeitszeit zu ziehen. Beachtlich in diesem Kontext ist vielmehr, dass die Verarbeitung von Standortdaten auch mit der Verarbeitung von besonderen personenbezogenen Daten i.S.d. Art. 9 Abs. 1 DSGVO einhergeht. So können bspw. Gesundheitsdaten bei regelmäßigen Besuchen in Krankenhäusern erhoben werden. Auch die sexuelle Orientierung lässt sich durch die Besuche entsprechender Orte nachvollziehen. Umstände wie diese können je nach Sektor, Branche sowie Angestelltenposition eklatante Folgen für den Beschäftigten haben. Per se wird die Verarbeitung solcher besonderen personenbezogener Daten mit einem psychischen Druck für den Beschäftigten verbunden, der für jenen ohne weitere Maßnahmen nicht tragbar ist. Festzuhalten ist vorerst, dass die Interessen der Beschäftigten grundsätzlich das Interesse des Verantwortlichen überwiegen. Nebst der Einhaltung der Datenschutzgrundsätze sind in diesem Fall daher dedizierte technische und organisatorische Maßnahmen (im Folgenden „TOM“) zu ergreifen, die die Folgen und Risiken für die Betroffenen minimieren.

2.4.1.2.2 Wahrung der Datenschutzgrundsätze

Bei der Verarbeitung von Standortdaten in PHEVs sind die fundamentalen Grundsätze Transparenz, Selbstbestimmung und Datensicherheit zu wahren.[100] Transparenz gegenüber dem Betroffenen schafft der Verantwortliche, wenn er diesen vollumfassend über die Datenverarbeitung, den Verarbeitungsumfang und -zweck sowie über die Dauer der Ver-

[98] Vgl. *Welthungerhilfe (Hrsg.)*, Naturkatastrophen und der Klimawandel.
[99] Vgl. *Schwarzer*, Plug-in-Hybridautos: Die Sogwirkung der Subventionen.
[100] Vgl. *Verband der Automobilindustrie (VDA) (Hrsg.)*, Drei Prinzipien für den Datenschutz beim autonomen und vernetzten Fahren.

arbeitung informiert.[101] Die notwendigen Informationen sind präzise, leicht zugänglich und verständlich sowie in klarer und verständlicher und einfacher Sprache anzufassen und gegebenenfalls zusätzliche visuelle Elemente zu verwenden, ErwGr. 58 DSGVO. Solche Informationen können in Form einer Datenschutzerklärung durch Integration in das Infotainmentsystem an entsprechenden Touchpoints übermittelt werden.[102] Der Europäische Datenschutzausschuss empfiehlt zudem, relevante Informationen in unterschiedlichen Kanälen und Medien zur Verfügung zu stellen („multi-channel"-Ansatz), welche in unterschiedlicher Form erfolgen können.[103] Diese Informationen und alle aktiven Funktionen sollten dem Kunden zudem in Echtzeit zur Verfügung stehen z.B. über eine in der App integrierte Funktionsanzeige gekennzeichnet durch standardisierte Symbole oder auch über das Cockpit im Fahrzeug.[104] Im Sinne der Datenhoheit sollte das Recht auf Widerspruch gegen die Datenverarbeitung ebenfalls technisch ermöglicht werden und simultan in das Infotainmentsystem etabliert sein. Von besonderer Bedeutung dabei ist der Grundsatz Privacy by Design nach Art. 25 Abs. DSGVO. Der besagt, dass jegliche datenschutzrechtlichen Anforderungen bereits während der Entwicklung der Fahrzeuge zu berücksichtigen sind.[105] Dabei sollte stets eine Datenverarbeitung innerhalb des Fahrzeugs erwogen werden, soweit dies technisch möglich ist. Im Hinblick auf die Programmierung von Datenspeicherung in den Steuergeräten ist zudem der Grundsatz der Datenminimierung zu beachten. Angesichts dessen, dass das Risiko für die Rechte und Freiheiten der betroffenen Personen auf das Mindeste zu minimieren ist, sind überdies adäquate Pseudonymisierungs- und Anonymisierungsmaßnahmen zu ergreifen.[106] Zu beachten gilt zudem gem. Art. 25 Abs. 2 DSGVO, dass in der Entwicklungsphase des Fahrzeuges auch Voreinstellungen entwickelt werden, die die Datenschutzkonformität unterstützen (sog. datenschutzfreundliche Voreinstellung, „Privacy by Default"). Um dem Grundsatz der Speicherbegrenzung und Datenminimierung genügend Rechnung zu tragen, sollten durch die Voreinstellungen die Daten nur im zwingend erforderlichen Umfang gespeichert werden – d.h. nach Zweckentfall und Ablauf einschlägiger Aufbewahrungsfristen sind die Daten zu löschen. Ferner ist in Erwägung zu ziehen, dass die Nutzung der PHEVs neben dem Beschäftigten auch durch andere Nutzer wie bspw. Familienmitglieder erfolgen kann. In diesem Fall sollten sowohl das Fahrzeug als auch die App über die Funktion verfügen, mehrere Nutzerprofile anzulegen oder mindestens anzugeben, dass ein anderer Nutzer das Fahrzeug fährt. Nach erfolgter Authentifizierung sollte es sodann möglich sein, die individuellen Datenschutzeinstellungen des Fahrers vor Fahrantritt zu aktivieren.[107] Hierbei ist die Datensicherheit stets unter Berücksichtigung des Stands der Technik zu gewährleisten. Bei einer Heranziehung der Einwilligung als Rechtsgrundlage sind die bereits beschriebenen Grundsätze ohne Einschränkung zu beachten.

---

[101] Vgl. *Wolff/Brink*, in: Beck`sche OK, Kapitel II Rn. 10.
[102] Vgl. *Leupold/Wiebe/Glossner* in: IT-Recht, Teil 10, D. II. Punkt 4 Rn. 39.
[103] Vgl. *European Data Protection Board (Hrsg.),* Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13.11.2019, Rn. 61.
[104] Vgl. *Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA) (Hrsg.)*, Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge, S. 3.
[105] Vgl. *European Data Protection Board (Hrsg.),* Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.
[106] Vgl. *Ottoschmidt,* Datenschutzrechtliche Empfehlungen zum automatisierten und vernetzten Fahren.
[107] Vgl. *Specht/Mantz/v. Bodungen*, in: Handbuch Europäisches und deutsches Datenschutzrecht, § 16 Rn. 46.

2.4.1.2.3 Notwendigkeit zur Durchführung einer Datenschutz-Folgenabschätzung

Risiken, die sich aus einer Verarbeitungstätigkeit für den Betroffenen ergeben, müssen mittels einer Datenschutz-Folgenabschätzung ermittelt werden. Hierzu ist eingangs zu prüfen, ob eine Datenschutz-Folgenabschätzung in diesem Fall vorausgesetzt wird. Die Prüfung erfolgt in mehreren Schritten und folgt einem dezidierten Schema.[108] Zuerst ist zu untersuchen, ob sich der betroffene Verarbeitungsvorgang auf der White-List nach Art. 35 Abs. 5 DSGVO befindet und diese somit von der Durchführung einer Datenschutz-Folgenabschätzung ausgenommen ist. Die Verarbeitung der Standortdaten im oben genannten Kontext findet sich nicht in der White-List nach Art. 35 Abs. 5 DSGVO wieder.[109] Insofern diese Verarbeitungstätigkeit von keiner White-List umfasst ist, ist im nächsten Schritt zu prüfen, ob die Verarbeitung auf der Black-List aufgeführt wird. Die Datenschutzkonferenz hat hierzu eine nicht abschließende Liste erstellt, die aufzeigt, welche Verarbeitungstätigkeiten einer Datenschutz-Folgenabschätzung unterzogen werden müssen.[110] Beachtlich hierbei ist, dass die Black-List Prozesse aufführt, die eine umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen zum Gegenstand haben.[111] Die Datenschutzkonferenz benennt dabei folgendes Beispiel: „Ein Unternehmen erhebt personenbezogene Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.“[112] Da die Funktionsweise von PHEVs analog zu den genannten Beispielen ist und Daten über den Aufenthalt natürlicher Personen verarbeitet werden, unterliegt diese Verarbeitungstätigkeit ebenso der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung.

2.4.2 Korrelation am Beispiel des Lieferkettensorgfaltspflichtengesetzes im Bereich Social

Die öffentliche Diskussion rund um die Einhaltung der Menschenrechte in der Lieferkette war mitunter der Grund dafür, dass der Bundestag am 11.6.2021 das geltende Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten („Lieferkettensorgfaltspflichtengesetz“, im Folgenden „LkSG“) beschloss.[113] Ziel dieses Gesetzes ist die Verhinderung von Kinderarbeit, Zwangsarbeit, Diskriminierung und mangelnden Sicherheitsstandards entlang der Lieferkette. Ferner sollen gewisse Standards für die Arbeitssicherheit aufrechterhalten werden, sodass Arbeitsunfälle und arbeitsbedingte Gesundheitsgefahren durch entsprechende Arbeitsbedingungen verhindert werden. Bemerkenswert ist zudem, dass das LkSG auch den Blick auf die ökologische Nachhaltigkeit richtet und auch die Abwendung von Umweltrisiken umfasst.

Grundlage für das Gesetzesvorhaben waren insbesondere die Leitprinzipien für Wirtschaft und Menschenrechte der UN.[114] Damit trägt das LkSG dem Menschenrechtsgedanken Rechnung, wodurch dieses und die in diesem Bereich ergriffenen Maßnahmen der Social-Dimension zuzuordnen sind. Auch in diesem Kontext sind Prozesse zu etablieren, die die

[108] Vgl. *GDD (Hrsg.)*, Voraussetzungen der Datenschutz-Folgenabschätzung, S. 6 ff.
[109] Vgl. *LDA Bayern (Hrsg.)*, Datenschutz-Folgenabschätzung.
[110] Vgl. *Datenschutzkonferenz (Hrsg.)*, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, S. 1 ff.
[111] Vgl. *Datenschutzkonferenz (Hrsg.)*, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, S. 1 ff.
[112] *Datenschutzkonferenz (Hrsg.)*, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, S. 2.
[113] Vgl. Bundesgesetzblatt, 2021, S. 2959.
[114] Vgl. *Leuering/Rubner*, NJW-Spezial, 399, 400.

Verarbeitung von zahlreichen Daten der (Sub-)Lieferanten zum Gegenstand haben[115], die einer datenschutzrechtlichen Würdigung zu unterziehen sind.

2.4.2.1 LkSG im Überblick

Das LkSG findet auf alle Unternehmen Anwendung, die ihren Hauptverwaltungs- oder Satzungssitz oder eine Zweigniederlassung in Deutschland haben. Des weiteren muss das Unternehmen in der Regel mindestens 3.000 Arbeitnehmer im Inland beschäftigen, davon umfasst sind auch ins Ausland entsandte Arbeitnehmer. Dieser Schwellenwert wird jedoch ab dem 1.1.2024 auf 1.000 Arbeitnehmer reduziert. Unternehmen, die vom Anwendungsbereich erfasst sind, müssen dezidierte Sorgfaltspflichten entlang der gesamten Lieferkette treffen. Dies reicht von der Rohstoffgewinnung bis hin zur Lieferung an den Endkunden im In- und Ausland, § 2 Abs. 5 Nr. 2 LkSG. Dabei differenziert das LkSG nicht zwischen Sektoren, Produkten oder Dienstleistungen, sondern gilt übergreifend und unabhängig von dem Unternehmensgegenstand.[116]

Im Überblick sind folgende Sorgfaltspflichten seitens der betroffenen Unternehmen einzuhalten:

- die Einrichtung eines Risikomanagements (§ 4 Abs. 1 LkSG),
- die Festlegung einer betriebsinternen Zuständigkeit (§ 4 Abs. 3 LkSG),
- die Durchführung regelmäßiger Risikoanalysen (§ 5 LkSG),
- die Verabschiedung einer Grundsatzerklärung (§ 6 Abs. 2 LkSG),
- die Verankerung von Präventionsmaßnahmen im eigenen Geschäftsbereich (§ 6 Abs. 1 und 3 LkSG) und gegenüber unmittelbaren Zulieferern (§ 6 Abs. 4 LkSG),
- das Ergreifen von Abhilfemaßnahmen (§ 7 Abs. 1 bis 3 LkSG),
- die Einrichtung eines Beschwerdeverfahrens (§ 8 LkSG),
- die Umsetzung von Sorgfaltspflichten in Bezug auf Risiken bei mittelbaren Zulieferern (§ 9 LkSG) und
- die Dokumentation (§ 10 Abs. 1 LkSG) und die Berichterstattung (§ 10 Abs. 2 LkSG) der Einhaltung der Sorgfaltspflichten.

Die Dokumentation der Einhaltung der Sorgfaltspflichten ist zu Nachweiszwecken sieben Jahre aufzubewahren. Die vom LkSG erfassten Unternehmen müssen zudem jährlich einen Bericht publizieren, der die Einhaltung der Sorgfaltspflichten des letzten Geschäftsjahres beinhaltet. Dieses ist spätestens vier Monate nach Geschäftsende zu veröffentlichen.[117] Daneben ist die Managementebene dazu verpflichtet, eine Grundsatzerklärung für die Menschenrechtsstrategie des Unternehmens abzugeben. Um die Effektivität zu erhöhen, muss das Unternehmen überdies eine angemessenes Beschwerdeverfahren einrichten, § 8 LkSG. Arbeitnehmern oder auch Außenstehenden wird auf diese Weise ermöglicht, Hinweise auf mögliche menschenrechts- oder umweltbezogene Risiken zu geben.

Bei einem Verstoß gegen die Sorgfaltspflichten drohen dem betroffenen Unternehmen erhebliche Bußgelder. Das Bundesamt für Wirtschaft und Ausfuhrkontrolle kann bei vorsätzlichen und fahrlässigen Verstößen gegen Vorschriften des LkSG Bußgelder von bis zu 800.000 Euro verhängen, bei Unternehmen mit einem Umsatz von mehr als 400 Mio. Euro aufgestockt auf bis zu zwei Prozent des globalen Umsatzes. Außerdem kann ein Unternehmen für einen Zeitraum von bis zu drei Jahren von der Vergabe öffentlicher Auf-

[115] Vgl. § 3 LkSG.
[116] Vgl. *Leuering/Rubner*, NJW-Spezial, 399, 400.
[117] Vgl. *Leuering/Rubner*, NJW-Spezial, 399, 400.

träge ausgeschlossen werden, wenn ein Bußgeld von 175.000 Euro oder mehr verhängt wird (§ 22 LkSG).

2.4.2.2 Datenschutzrechtliche Implikationen

Wie bereits oben aufgeführt, sind Unternehmen verpflichtet, ein Risikomanagement zur Überwachung ihrer Lieferketten einzurichten. Das Risikomanagement muss die gesamte Lieferkette erfassen und in allen maßgeblichen (unternehmensinternen) Geschäftsprozessen involviert sein (§ 4 LkSG). In der Regel kann mit einer Risikoanalyse, die auch Lieferantendaten zum Gegenstand hat, auch die Verarbeitung von personenbezogenen Daten einhergehen. Dies gibt Anlass dazu, die Durchführung einer Risikoanalyse der datenschutzrechtlichen Bewertung zu unterziehen.

2.4.2.2.1 Lieferketten-Risikoanalyse und Verarbeitung von Lieferantendaten

Eine höhere Bedeutung im Kontext des Datenschutzes hat jedoch die Tatsache, dass Unternehmen nach § 5 LkSG eine Risikoanalyse durchführen müssen, die der Ermittlung von menschenrechts- und umweltbezogenen Risiken dienen soll. Hierzu schreibt § 5 Abs. 4 LkSG mindestens eine jährliche Prüfung der unmittelbaren Zulieferer im eigenen Geschäftsbereich vor. Daneben müssen zusätzlich anlassbezogene Prüfungen bei wesentlich veränderter oder erweiterter Risikolage unternommen werden, die ermitteln, ob eine Verletzung der Menschenrechte oder Umweltstandards vorliegt. Bei mittelbaren Zulieferern besteht die Pflicht zur Risikoanalyse nur, wenn das Unternehmen substanziierte Kenntnis von möglichen Verletzungen hat. Wenn Unternehmen ein Risiko feststellen, müssen unverzüglich angemessene Präventionsmaßnahmen ergriffen und diese jährlich sowie anlassbezogen überprüft werden (§ 6 Abs. 1 und 5 LkSG). Stellt das Unternehmen sodann Verletzungen fest, hat es Abhilfemaßnahmen zu treffen. Ultima ratio kann auch der Abbruch der Geschäftsbeziehung zu dem Zulieferer sein. Zur Durchführung der Prüfung und der Risikoanalyse werden Daten zu den Lieferanten und dessen Beschäftigten benötigt, die eine effektive Risikoanalyse und -einschätzung ermöglichen. Solche Daten umfassen auch sog. Lieferantendaten, die ebenfalls einen Personenbezug aufweisen können und von Art. 4 Abs. 1 DSGVO umfasst sind, insofern es sich dabei nicht um juristische Personen handelt.[118] Dies ist bspw. dann der Fall, wenn konkrete Ansprechpartner zugeteilt sind und dessen Vor- und Nachname in diesem Zusammenhang verarbeitet werden. Überdies werden zur Risikobewertung und -analyse unterschiedliche Mittel fällig, wie etwa der Einsatz von Selbstauskunftsbögen, in denen auch Auskunft zu früheren Menschenrechtsverletzungen oder Nichteinhaltung von Umweltstandards und die hiervon betroffenen Personen verlangt werden. Ferner sind auch Gespräche mit den Ansprechpartnern nötig, die im Anschluss dokumentiert werden müssen und damit auch personenbezogene Daten enthalten.[119] Daher fallen auch diese Daten in den Anwendungsbereich der DSGVO, wodurch in der Verarbeitung der Lieferantendaten ebenfalls die Grundsätze der DSGVO verankert sein müssen.

2.4.2.2.2 Etablierung eines Beschwerdeverfahrens (Hinweisgebersystem)

Von zentraler Bedeutung ist es zudem, dass nach § 8 LkSG ein angemessenes Beschwerdeverfahren durch die Unternehmen einzuführen ist. Dies bedeutet, dass das Hinweisgebersystem es Personen ermöglichen soll, Risiken bezogen auf Menschenrechte oder Umwelt und Menschenrechtsverletzungen oder Verletzungen der Umweltstandards zu melden, die durch das wirtschaftliche Handeln eines Unternehmens im eigenen Ge-

[118] Vgl. Bekanntmachung des Innenministeriums Baden-Württemberg über Hinweise (Nr. 38) zum Bundesdatenschutzgesetz für die private Wirtschaft vom 18.1.2000.
[119] Vgl. *WEKA (Hrsg.)*, Lieferkettengesetz: praktische Umsetzung in Unternehmen.

schäftsbereich oder eines unmittelbaren Zulieferers entstanden sind. Das Verfahren muss potenziellen Beteiligten zugänglich sein, Vertraulichkeit wahren und wirksamen Schutz vor Benachteiligung oder Bestrafung aufgrund einer Beschwerde gewährleisten.[120]

Beachtlich ist jedoch, dass in nahezu allen Meldungen, die im Hinweisgebersystem eingehen, ein Personenbezug besteht.[121] Für die Meldung und Nachverfolgung erforderlich sind grundsätzlich der Name des Hinweisgebers und der beschuldigten bzw. involvierten Personen. Daneben werden auch weitere Informationen mit Personenbezug wie etwa die Mitarbeiterfunktion im Unternehmen und die Umstände der Beobachtung erfasst.[122] Der nächste Schritt im Meldeprozess beinhaltet einen sog. Plausibilitätscheck, in der die Daten der initialen Prüfung erfasst werden. Im Rahmen des Plausibilitätschecks werden weitere personenbezogene Daten aus (IT-)Systemen und Datenbanken (z.B. Reisekostenabrechnung) herangezogen und evaluiert, um die Angaben zu überprüfen.[123] Ergibt die initiale Prüfung, dass der Sachverhalt und damit der Verstoß plausibel ist, müssen weitere personenbezogene Daten (z.B. E-Mails und Messengerdienste) auf Grundlage einer forensischen (Daten-)Analyse untersucht und bewertet werden. Je nach Ergebnis der Zweitprüfung erfolgt eine Rückmeldung an den Hinweisgeber mit Informationen zum aktuellen Stand. Daraufhin werden sachverhaltsaufklärende Interviews u.a. mit den beschuldigten Personen durchgeführt und in einem Bericht dokumentiert, der wiederum an die Geschäftsführung/den Vorstand berichtet wird.[124] Im Rahmen des Hinweisgebersystems ist von dem folgenden Datenfluss von personenbezogenen Daten auszugehen:

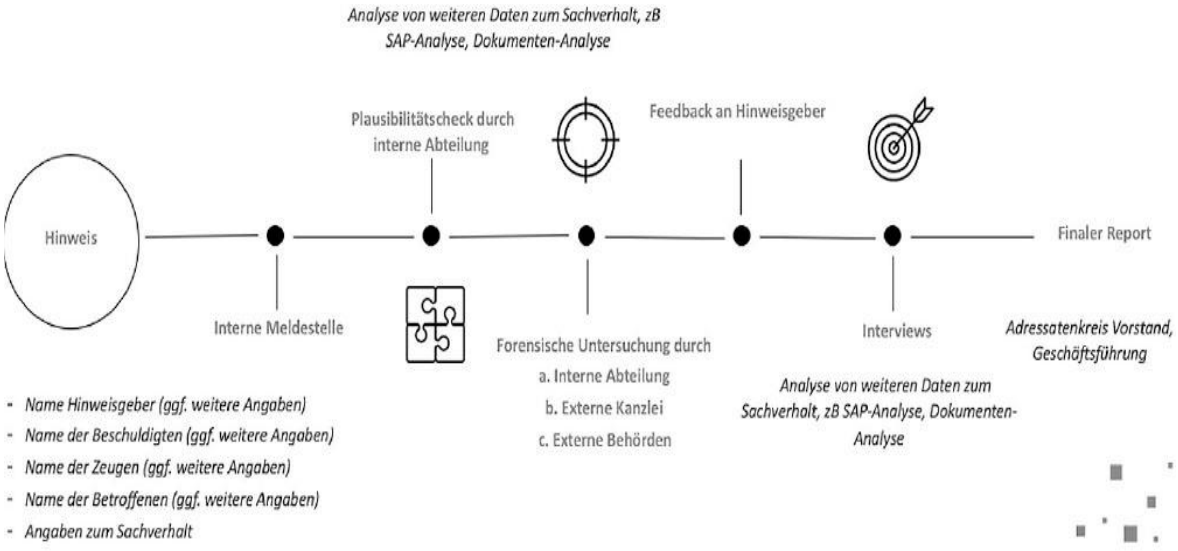

Abbildung 5: Whistleblowing und Datenschutz – ein unlösbares Spannungsfeld?

Fehr, ZD 2022, 256, 260.

Da im Rahmen einer solchen Meldung im Sinne des LkSG eine Vielzahl und insbesondere auch besondere personenbezogene Daten anfallen, ist der Anwendungsbereich der

[120] Vgl. *Stöbener de Mora/Noll*, NZG, 1237, 1244.
[121] Vgl. *Fehr,* ZD 2022, 256, 256.
[122] Vgl. *Datenschutzkonferenz (Hrsg.),* Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, S. 4.
[123] Vgl. *Fehr*, ZD 2022, 256, 256.
[124] Vgl. *Fehr*, ZD 2022, 256, 256.

DSGVO nach Art. 4 Abs. 1 eröffnet. Damit sind alle Anforderungen und Verpflichtungen bei der Verarbeitung dieser Daten zu berücksichtigen.

2.4.2.3 Lösung des Spannungsfeldes LkSG und Datenschutz

Beide Gesetzgebungen sehen exorbitante Bußgelder im Falle eines Verstoßes vor. Es mag eher wenig zielführend sein, die Anforderungen der LkSG zu erfüllen, während jene der DSGVO missachtet werden. Andersrum drohen auch bei einem Verstoß gegen das LkSG eklatante Bußgelder. Die Herausforderung besteht demnach darin, beide Regelwerke in Einklang zu bringen und damit das Risiko eines Bußgeldes aus beiden Perspektiven zu minimieren. Es ist also unabdingbar dieses Spannungsfeld durch geeignete datenschutzrechtliche Maßnahmen zu lösen.

2.4.2.3.1 Rechtmäßigkeit der Verarbeitung

Die Verarbeitung von personenbezogenen Daten des Hinweisgebers kann sich grundsätzlich aus Art. 6 DSGVO, einer Kombination aus Art. 6 DSGVO mit anderen Normen wie bspw. der Whistleblower-Richtlinie[125], einer Kollektivvereinbarung oder der Einwilligung der betroffenen Personen ergeben.[126] Bisher kam eine Rechtmäßigkeit der Verarbeitung aufgrund einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 lit. c) DSGVO nicht in Betracht – bis auf ausgewählte Sektoren, z.B. Banken, Versicherungen, Krankenversicherungen, da es an einer rechtlichen Verpflichtung als solche gemangelt hat. Dieser Umstand ändert sich jedoch für die Unternehmen, die vom LkSG betroffen sind. Da § 8 LkSG eine Verpflichtung für Unternehmen bereithält, ein Beschwerdeverfahren zu etablieren, kann die Verarbeitung personenbezogener Daten im Rahmen des Meldekanals auf Art. 6 Abs. 1 lit. c) DSGVO gestützt werden.

2.4.2.3.2 Informationspflichten

Nachdem personenbezogene Daten sowohl über den Hinweisgeber als auch über die beschuldigte Person verarbeitet werden, ist der Grundsatz der Transparenz zu wahren und damit die Informationspflichten aus Art. 14 DSGVO zu erfüllen. Dies stellt insbesondere in diesem Kontext eine Herausforderung dar. Nach Art. 14 Abs. 3 lit. a DSGVO ist die beschuldigte Person spätestens einen Monat ab Erhalt der Meldung zu informieren. Beachtlich ist jedoch, dass Informationen über die Datenverarbeitung an die beschuldigte Person, die Ermittlungen erschweren oder sogar diese gefährden können. Hierfür hält Art. 14 Abs. 5 DSGVO jedoch die Ausnahme bereit, die Frist der Informationspflicht gemäß Art. 14 Abs. 5 lit. b DSGVO zu verlängern, solange eine Verdunklungsgefahr bestätigt und die Beweise nicht vollends gesichert sind. Allerdings reicht die Verlängerung der Frist in der Regel nicht, bis die Ermittlungen und die Aufklärung des Sachverhalts abgeschlossen sind.[127] Dieser Aspekt hat eine zentrale Bedeutung im Kontext eines Beschwerdeverfahrens; denn hier geraten der Schutz des Hinweisgebers und das Auskunftsrecht der beschuldigten Person in Konflikt. Anlässlich dessen, dass eine Offenlegung der Identität des Hinweisgebers eher zu einem Rückgang der getätigten Meldungen führt und dadurch die Vertraulichkeit gegenüber jenem zu wahren ist, ist eine Auskunft an die beschuldigte Person über die Identität des Hinweisgebers zu verneinen.[128] Damit weder eine zu frühe Unterrichtung der beschuldigten Person stattfindet noch eine verzögerte Unterrichtung – die folglich Bußgelder zur Folge hat – müssen genügend Informationen vorliegen, sodass die

[125] Vgl. Richtlinie (EU) des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden.
[126] Vgl. *Datenschutzkonferenz (Hrsg.)*, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, S. 6.
[127] Vgl. *Fehr*, ZD 2022, 256, 258.
[128] Vgl. *Fehr*, ZD 2022, 256, 258.

Sachverhaltsaufklärung nicht gefährdet wird. Eine Unterrichtung der betroffenen Personen ist demnach dann sinnvoll, nachdem die ersten forensischen Datenanalysen im Rahmen der sachverhaltsaufklärenden Gespräche stattgefunden haben.[129]

2.4.2.3.3 Auskunftsanspruch der beschuldigten Person

Relevant ist darüber hinaus, welche Wechselwirkungen zwischen dem Auskunfts- und Kopieanspruch der beschuldigten Person(en) aus Art. 15 Abs. 1 Hs. 2 und Abs. 3 DSGVO entstehen. Das Recht bezieht sich auf alle Informationen über die Herkunft der Daten und eröffnet somit ein Spannungsverhältnis zur zugesicherten Vertraulichkeit der Identität des Hinweisgebers. Zum Auskunftsanspruch in Bezug auf Hinweise Dritter im Meldekanal bezog bereits das Landesarbeitsgericht Baden-Württemberg am 20.12.2018 Stellung.[130] Dieses beschloss, dass betroffene Personen grundsätzlich einen Anspruch auf Einsicht in die Verarbeitung personenbezogener Daten im Kontext einer Meldung haben. Ob und inwiefern der beschuldigten Person Auskunft über den Hinweisgeber erteilt wird, hängt maßgeblich von der Form der Geheimhaltungsverpflichtung ab. Liegt der Geheimhaltungsverpflichtung lediglich eine Vereinbarung und keine gesetzliche Verpflichtung zugrunde, ist eine Abwägung zwischen dem Interesse des Hinweisgebers an Vertraulichkeit und Geheimhaltung sowie dem Auskunftsinteresse der betroffenen Personen vorzunehmen. Diese Interessensabwägung ist beiden Parteien offenzulegen und zu begründen.[131] Mit der Fragestellung, wie umfassend dem Auskunftsanspruch und Kopieanspruch nachgekommen werden muss, befasste sich mehrmals das BAG[132]. Eine Anfrage der beschuldigten Person auf Aushändigung solcher Kopien – im Streitfall insbesondere von E-Mails – müsse dezidiert bezeichnet werden.[133] Im Beschäftigungskontext haben bspw. Mitarbeiter nach Art. 15 Abs. 3 DSGVO demzufolge keinen uferlosen Anspruch auf Aushändigung der Kopien; vielmehr unterliegt dem Ganzen ein abgestuftes Verfahren, wonach Kopien nur nach bestimmten Informationen zu übermitteln sind. Schutzzweck des Art. 15 Abs. 3 DSGVO ist es den Auskunftsanspruch zu prüfen, was folglich zu einer Beschränkung des Kopieranspruchs führt.[134] Maßgabe ist daher die Bestimmtheit des Kopieanspruches – und ist somit an den Auskunftsanspruch nach Art. 15 Abs. 1 DSGVO gekoppelt. Im Übrigen kann der Kopieanspruch vom Verantwortlichen abgewiesen werden, wenn die Voraussetzung der Bestimmtheit nicht gegeben ist. Zu beachten ist indessen, dass stets die Vorgaben zur Geheimhaltung der Identität und Vertraulichkeit des Hinweisgebers gewahrt werden müssen.[135]

2.4.2.3.4 Durchführung einer Datenschutz-Folgenabschätzung

Vor der Einführung des Beschwerdeverfahrens ist zusätzlich die Notwendigkeit zur Durchführung der Datenschutz-Folgenabschätzung zu prüfen. Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, auf Grund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, ist von dem Verfahrensverantwortlichen vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für

[129] Vgl. *Fehr*, ZD 2022, 256, 258.
[130] Vgl. LAG Baden-Württemberg, Urteil vom 20.12.2018 – 17 Sa 11/18 (ArbG Stuttgart); nicht rechtskräftig, ZD 2019, 276, mAnm Wybitul.
[131] Vgl. *Fehr*, ZD 2022, 256, 259.
[132] Vgl. u.a. BAG, Urteil vom 27.04.2021 – Az. 2 AZR 342/20, ZD 2021, 589, 591; BAG, Urteil vom 16.12.2021 – Az. 2 AZR 235/21, Legal Tribune Online.
[133] Vgl. u.a. BAG, Urteil vom 27.04.2021 – Az. 2 AZR 342/20, ZD 2021, 589, 591; BAG, Urteil vom 16.12.2021 – Az. 2 AZR 235/21, Legal Tribune Online.
[134] Vgl. *Fehr*, ZD 2022, 256, 259.
[135] Vgl. *Fehr*, ZD 2022, 256, 259.

den Schutz personenbezogener Daten durchzuführen, Art. 35 Abs. 1 DSGVO.[136] Zweck eines solches Beschwerdeverfahrens ist es u.a. Meldungen über vermutliche Verstöße gegen geltende Gesetze zu tätigen und daraufhin zu erfassen. Neben den gesetzlichen Sanktionen drohen den betroffenen Personen (u.a. Hinweisgeber, beschuldigte Person, Zeugen etc.) weitere schwerwiegende Konsequenzen und müssen Repressalien fürchten. So ist auch mit arbeitsrechtlichen Maßnahmen oder öffentlicher Kritik zu rechnen, wenn der Sachverhalt öffentlichkeitswirksam wird. Es besteht somit ein besonderes Risiko für die Rechte und Freiheiten der betroffenen Personen. Ein Beschwerdeverfahren mit seinem Meldeprozess unterliegt folglich einer Datenschutz-Folgenabschätzung gem. Art. 35 Abs. 1 DSGVO.

2.4.2.3.5 Löschung der Daten

Fraglich ist zudem, wie sich die Ermittlungen und damit die Speicherung der Beweismittel mit dem Grundsatz der Speicherbegrenzung und Datenminimierung verhält. Hierbei geraten das Dokumentationserfordernis aus § 10 LkSG und die Löschpflicht aus Art. 17 Abs. 1 DSGVO in Kollision. Grundsätzlich sieht § 10 LkSG eine Aufbewahrungspflicht von mindestens sieben Jahren ab Erstellung vor. Diese Frist erscheint jedoch im Kontext eines Meldekanals fragwürdig, zumal sich der Wortlaut der Norm lediglich auf die Dokumentation zur Erfüllung der Sorgfaltspflichten bezieht. Daneben sieht die Datenschutzkonferenz in ihrer Orientierungshilfe zur Whistleblower-Hotline eine Löschung nach zwei Monaten nach Abschluss der Ermittlungen als angemessen, insofern weitere rechtliche Schritte wie die Einleitung eines Strafverfahrens nicht erforderlich sind.[137] Die Herausforderung in der Praxis besteht demnach darin, den Sachverhalt dann abzuschließen, wenn genügend Beweismittel vorliegen, jedoch auch nicht das Recht auf informationelle Selbstbestimmung der Betroffenen zu strapazieren. Ursache hierfür ist, dass erst zu einem späteren Zeitpunkt weitere Beweise und Hinweise z.B. durch einen anderen Hinweisgeber eingereicht oder sogar durch Dritte an das Unternehmen herangetragen werden, z.B. die Medien oder externe Ermittler.[138] Eine Ausnahme ist jedoch in Art. 17 Abs. 3 lit. e) DSGVO wiederzufinden. Die Norm sieht vor, dass personenbezogene Daten nach Zweckentfall dann nicht zu löschen sind, wenn diese die Geltendmachung eigener Rechtsansprüche sowie die Verteidigung gegen Rechtsansprüche Dritter sichern. Dies dürfte bspw. der Fall sein, indem ein benachteiligendes Beweismittel infolge der Löschungsverpflichtung verhindert wird.[139] Das Beweisinteresse besteht so lange wie mit der Geltendmachung von Ansprüchen zu rechnen ist. Zur Bestimmung der Löschfrist können somit die Verjährungsfristen aus § 195 Bürgerliches Gesetzbuch (im Folgenden: BGB) als Aufbewahrungsfrist herangezogen werden. § 195 BGB setzt die Frist der Verjährung von Rechtsansprüchen auf drei Jahre. Um jedoch das Recht Schutz der personenbezogenen Daten nicht zu überspannen, ist es ratsam, die personenbezogenen Daten in einem gestuften Verfahren in der ersten Phase zu pseudonymisieren, daraufhin zu anonymisieren und anschließend zu löschen. Jedoch unter der Prämisse, dass die Merkmale des Sachverhalts, die Beweismittel und der Sachverhalt selbst ausreichend dokumentiert sind.

[136] Vgl. *Datenschutzkonferenz (Hrsg.)*, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, S. 12.
[137] Vgl. *Datenschutzkonferenz (Hrsg.)*, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, S. 12.
[138] Vgl. *Fehr*, ZD 2022, 256, 259.
[139] Vgl. *Fehr*, ZD 2022, 256, 259.

2.4.3 Einsatz von Google Analytics zur Analyse des Nutzerverhaltens im Bereich Governance

Unternehmen streben auf eine Maximierung des Shareholder-Values hin, die eine Interpendenz zur Kundenzufriedenheit aufweist. Hierzu ist es notwendig, die Bedürfnisse der eigenen Zielgruppe bestmöglich zu kennen auf Grundlage einer umfangreichen Datenauswertung. Vor diesem Hintergrund ist der Einsatz von Webanalyse-Tools für viele Betreiber unerlässlich. Google Analytics ist dabei ein im Markt fest etabliertes Tool, was für viele Unternehmen zum festen Bestandteil digitaler Vermarktungskonzepte gehört. Das Webanalyse-Tool ermöglicht es Unternehmen Informationen über das Nutzerverhalten und die Zugriffe auf die eigene Webseite zu sammeln und auszuwerten. Auf Grundlage dieser Informationen können Unternehmen Optimierungsmaßnahmen ergreifen, um gezielteres Marketing zu betreiben, sodass die Profitabilität und damit der Shareholder-Value gesteigert werden können. Allerdings kollidiert der Einsatz jenes Tools oft mit der Social-Komponente, da Google aufgrund seiner Datenschutzpraktiken häufig in Kritik gerät.[140]

2.4.3.1 Funktionsweise von Google Analytics

Für die Funktionsweise wird im ersten Schritt jeder Webseite ein Tracking-Code für das Page-Tagging zugewiesen (sog. Google Analytics Tracking Code, im Folgenden: GATC). Der GATC befindet sich im Header eines HTML-Dokuments.[141] Ruft somit ein Nutzer die Webseite auf, werden über den Tracking-Code Interaktionen mit der Seite gesammelt. Gelangt der Nutzer auf die Webseite, wird der GATC ausgeführt und es wird eine Verbindung zum Google Analytics Server hergestellt. Unterdessen werden bereits vorhandene Daten vom Client ausgelesen (Browser-Anbieter, Browser-Version, Sprache, etc.). und gleichzeitig Cookies auf dem Gerät platziert, worauf sich die Informationen vom Client befinden. Nebenbei lädt der Browser die Datei „ga.js“ von einem Google Analytics Server herunter. Sobald die Datei heruntergeladen wurde, findet eine Versendung der Daten an den Google Analytics Server mittels eines „Pageview“ statt.[142] Damit findet die Kommunikation zum Server statt, in der mitgeteilt wird, dass die Webseite von dem User gesichtet wurde. Es können aber noch eine Vielzahl von anderen Daten übertragen werden:[143]

- Die IP-Adresse des Nutzers[144],
- einzigartige Online-Kennungen („unique identifier“), die sowohl den Browser bzw. das Gerät des Besuchers als auch den Website-Betreiber identifizieren[145];
- Eigenschaften des Rechners und Informationen zum Browser des Besuchers z.B. Chrome, Firefox;
- Spracheinstellung, das Gerät und das Betriebssystem des Besuchers z.B., iOS, Windows, Android[146];
- Informationen zum Besucher: Herkunft des Besuchers, Häufigkeit des Besuches dieses Gerätes, Datum und Zeitpunkt des Besuchs;

---

[140] Vgl. *Deiwick*, ZD 2022, 01125.
[141] Vgl. *Hofstätter,* in: Werbe- und Kommunikationsforschung, Kapitel 11: Logfile-Analyse und Google Analytics, S. 191.
[142] Vgl. *Hofstätter,* in: Werbe- und Kommunikationsforschung, Kapitel 11: Logfile-Analyse und Google Analytics, S. 191.
[143] Vgl. *Hofstätter,* in: Werbe- und Kommunikationsforschung, Kapitel 11: Logfile-Analyse und Google Analytics, S. 191.
[144] Vgl. *Deiwick*, ZD 2022, 01125.
[145] Vgl. Österreichische Datenschutzbehörde, Bescheid vom 22.12.2021, D155.027 2021-0.586.257, S. 18, Spruchpunkt C. 9.
[146] Vgl. *Google (Hrsg.)*, Funktionsweise von Google Analytics.

- Quelle des Besuchers: Wie ist der Besucher auf die Website gelangt? Z.B. Suchbegriff, eine Anzeige oder E-Mail-Marketingkampagne[147];
- Seiteninformationen: URL und Page Title der aufgerufenen Seite;
- E-Commerce-Informationen: Gekaufte Produkte, Produktpreise, Kaufvolumen etc.

So kann das Unternehmen bspw. nachvollziehen, wie viele Nutzer eine Seite mit Trinkgefäßen und wie viele eine Seite für Haushaltswaren besucht haben.[148] Google Analytics segmentiert die Daten daraufhin in einzelne Felder sowie Dimensionen und ordnet diese bestimmten Attributen zu, die anschließend in einem Bericht zusammengefasst werden. Abschließend werden die Daten und die Ergebnisse der Auswertungen auf einer Datenbank gespeichert, welche dann über die Benutzerfläche im Google-Analytics Account des Unternehmens eingesehen werden können.[149]

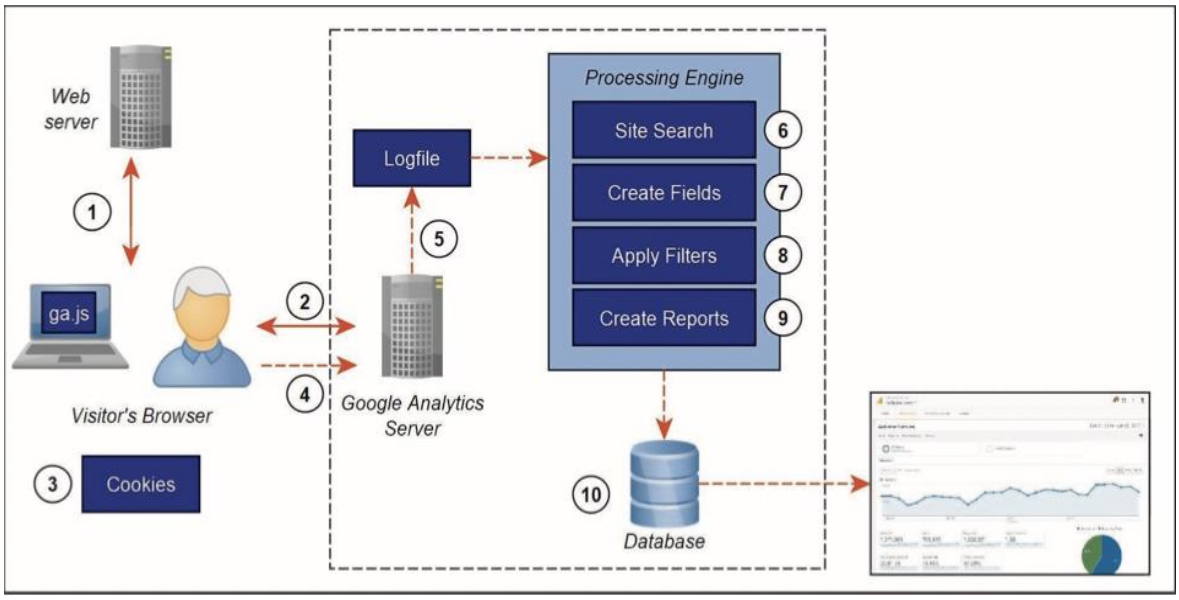

Abbildung 6: Funktionsweise von Google Analytics.

U.a. Hofstätter, in: Werbe- und Kommunikationsforschung, Kapitel 11: Logfile-Analyse und Google Analytics, S. 191.

2.4.3.2 Kollisionen des Tools mit dem Datenschutz

Der Einsatz von Google Analytics ist in vielerlei Hinsichten mit datenschutzrechtlichen Bedenken versehen. Jedoch finden diese seinen Ursprung bereits in der Definition und Auslegung des Begriffs personenbezogener Daten i.S.d. Art. 4 DSGVO. Während Google der Auffassung ist, dass es sich bei den oben benannten Daten nicht um personenbezogene Daten handelt nach Art. 4 Abs. 1 DSGVO[150], widersprechen dem die Datenschutzbehörden. Folgerichtig argumentieren letztere, der Umstand allein genüge, dass die oben

[147] Vgl. *Google (Hrsg.)*, Funktionsweise von Google Analytics.
[148] Vgl. *Google (Hrsg.)*, Funktionsweise von Google Analytics.
[149] Vgl. *Hofstätter, in*: Werbe- und Kommunikationsforschung, Kapitel 11: Logfile-Analyse und Google Analytics, S. 191.
[150] Vgl. Google stuft personenidentifizierbare Daten als Daten ein, durch die allein eine natürliche Person direkt identifiziert, kontaktiert oder genau geortet werden kann, *Google (Hrsg.)*, Google Analytics-Hilfe.

benannten Daten zur Identifizierung von Einzelpersonen herangezogen werden können, um den Anwendungsbereich der DSGVO zu eröffnen.[151] Beachtlich ist zudem, dass die Rechtmäßigkeit der Verarbeitung der Daten durch Google-Analytics zu Webanalysezwecken beschränkt ist. Eine Rechtmäßigkeit nach Art. 49 Abs. 1 lit. b) DSGVO zur Vertragserfüllung kommt nicht in Betracht, da die Datenverarbeitung nicht zur Erfüllung des Vertrages mit dem Nutzer notwendig ist. Zumal es in vielen Fällen bereits am Bestehen eines Vertragsverhältnisses mit dem Nutzer scheitert. Die Verarbeitung kann auch nicht auf das berechtigte Interesse (Art. 49 Abs. 1 lit. c) DSGVO) des Verantwortlichen gestützt werden, da die Interessen, Grundrechte und Grundfreiheiten der Nutzer regelmäßig die Interessen der Website-Betreiber überwiegen.[152] Demzufolge dürfte die Verarbeitung nur auf Grundlage einer Einwilligung des Nutzers nach Art. 49 Abs. 1 lit. a) i.V.m. Art. 7 DSGVO in Frage kommen. Dem widersprechen jedoch die Datenschutzbehörden unter dem Gesichtspunkt, dass es sich bei Art. 49 Abs. 1 lit. a) DSGVO um eine Ausnahmevorschrift handelt, die naturgemäß nicht die Rechtsgrundlage für eine regelmäßige und massenhaft durchgeführte Datenübermittlung in ein Drittland sein kann.[153] Abschließend ist somit schon die Rechtmäßigkeit der Verarbeitung durch Google Analytics fraglich, wodurch der Einsatz dessen nur in Ausnahmefällen stattfinden sollte.

2.4.3.2.1 Datentransfer ins Drittland und der Sturz des Privacy-Shields

Der Europäische Gerichtshof stürzte mit dem Urteil vom 16.7.2020 (Schrems II-Urteil) die informelle Absprache zwischen der EU und den USA (sog. „Privacy Shield“) und erklärte damit den Angemessenheitsbeschluss für ungültig.[154] Womit auch die bisherige Rechtsgrundlage für Datenübermittlungen in die USA wegfällt. D.h. es werden weitere „geeignete Garantien“ für die rechtmäßige Datenübermittlung in die USA notwendig. Dies stellt für Google-Analytics ein schwerwiegendes Problem dar, da Google Analytics personenbezogene Daten auf Cloud-Rechenzentren in den USA speichert, wodurch eine Datenübermittlung in ein unsicheres Drittland zweifelsohne stattfindet. Erschwerend kommt hinzu, dass „geeignete Garantien“ nach Art. 46 DSGVO nur bedingt eine Lösung darstellen. Geeignete Garantien könnten Standarddatenschutzklauseln (im Folgenden: SDK) nach Art. 46 Abs. 2 lit. c) DSGVO sein. Gleichwohl gelten in den USA Überwachungsgesetze (z.B. Cloud Act), die den lokalen Behörden Zugriffsrechte auf sämtliche Unternehmens- und Kundendaten von Unternehmen einräumen. Hiervon wird Google-Analytics auch umfasst und unterliegt somit diesen Regularien. Anlässlich dessen, dass die SDK ausschließlich im Verhältnis Verantwortlicher und Google-Analytics gelten und kaum bis wenig Bindungswirkung für die US-amerikanischen Behörden haben, scheinen diese ebenfalls ins Leere zu laufen.[155] Google-Analytics fungiert überdies als Auftragsverarbeiter. Für eine rechtmäßige Datenübermittlung an Auftragsverarbeiter ist es erforderlich, dass dieser

[151] Vgl. *Deiwick*, ZD 2022, 01125; *Datenschutzkonferenz (Hrsg.)*, Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich, S. 2.

[152] Vgl. *Datenschutzkonferenz (Hrsg.)*, Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich, S. 3.

[153] Vgl. *Deiwick*, ZD 2022, 01125; u.a. *Datenschutzkonferenz (Hrsg.)*, Orientierungshilfe der Aufsichtsbehörden für Anbieter*innen von Telemedien ab dem 1. Dezember 2021, S. 32; *Europäischer Datenschutzausschuss (Hrsg.),* Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, S. 4.

[154] Vgl. EuGH, Urteil vom 16.7.2020 – C-311/18, NJW 2020, 2613, 2613.

[155] Vgl. *Sourcing International (Hrsg.)*, Die Nutzung von Google Analytics ist nicht datenschutzkonform – Neue Grundsatzentscheidung der österreichischen Datenschutzbehörde.

technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten ergreift. Allerdings sind diese auf Seiten Google-Analytics nicht gegeben.[156]

2.4.3.2.2 Unzureichende Kürzung der IP-Adresse

Die erhobenen Daten werden zu Marketingzwecken gesammelt und ausgewertet. Daneben werden diese Daten auch mit Daten von anderen Quellen kombiniert und daraufhin Nutzerprofile erstellt, wodurch es möglich ist, einzelne Nutzer zu identifizieren. Um dem Datenschutzgedanken in einer Hinsicht Rechnung zu tragen, existiert die Möglichkeit, im Trackingcode eine Kürzung der IP-Adresse vorzunehmen, wodurch die IP-Adresse pseudonymisiert wird.[157] Demgegenüber sieht die österreichische Datenschutzbehörde die Pseudonymisierung der IP-Adressen nicht als ausreichend an, um die Identifizierung der betroffenen Personen zu verhindern.[158] Kritisch ist dabei vor allem, dass die IP-Adresse vollständig erhoben und als solche an Google-Analytics übermittelt wird. Erst im darauffolgenden Schritt findet die Kürzung der IP-Adresse statt. Zudem werden bei der Pseudonymisierung weitere Daten des Nutzers erfasst und gesammelt.[159]

2.4.3.2.3 Handlungsempfehlung zur Lösung des Spannungsfeldes Governance und Social

Im März 2022 verkündeten die EU-Kommission und die US-Regierung, dass aktuell Bemühungen für einen neuen Data-Privacy-Framework unternommen werden.[160] Das „Trans-Atlantic Data Privacy Framework“ könnte ein sicheres Abkommen zwischen den Parteien darstellen und den Datentransfer in die USA wieder legitimieren. Er umfasst Regelungen und verbindliche Garantien, wonach die Zugriffsrechte der US-Sicherheitsbehörden auf personenbezogene Daten auf ein zum Schutz der nationalen Sicherheit erforderliches Maß beschränkt werden.[161] Dennoch ist es nicht empfehlenswert, die weiteren Absprachen abzuwarten und keine Maßnahmen zu ergreifen. Denn bei einem Verstoß gegen die DSGVO drohen nach Art. 83 Abs. 5 DSGVO von bis 20.000.000 Euro Bußgeld. Aktuell wird jedoch den Verantwortlichen geraten, sich nach datenschutzkonformen Alternativen umzusehen, welche bspw. ihren Rechenzentren und Sitz in der Europäischen Union haben. Nur auf diese Weise lassen sich die Governance und Social-Dimensionen vereinen, ohne dabei auf die Maximierung des Shareholder-Values zu verzichten und das Recht auf informationelle Selbstbestimmung der betroffenen Personen zu gefährden.

2.5 ESG-Score und die Berücksichtigung des Datenschutzes im Bewertungsverfahren

Den Datenschutz allein auf abstrakter Ebene als integralen Bestandteil aufzunehmen, genügt nicht, um eine effektive Umsetzung zu realisieren. Denn Peter F. Drucker zitierte einst „Was man nicht messen kann, kann man nicht lenken.“, was an Allgemeingültigkeit gewonnen hat und somit auch für den Datenschutz gelten dürfte. Im Kontext ESG bedeutet dies, dass die Ratingagenturen Risiken, die sich für das Unternehmen aus dem Datenschutz ergeben, berücksichtigen müssen, um dem Bedürfnis der Investoren nachzukommen. Das Risiko, das sich aus dem Datenschutz für das jeweilige Unternehmen ergibt, muss demnach ermittelt werden, sodass die Ratingagenturen das Risiko evaluieren und

[156] Vgl. Österreichische Datenschutzbehörde, Bescheid vom 22.12.2021, D155.027 2021-0.586.257, S. 18, Spruchpunkt C. 9.
[157] Vgl. *Deiwick*, ZD 2022, 01125.
[158] Vgl. *Deiwick*, ZD 2022, 01125.
[159] Vgl. *Deiwick*, ZD 2022, 01125.
[160] Vgl. *Europäische Kommission (Hrsg.)*, Gemeinsame Erklärung der Europäischen Kommission und der Vereinigten Staaten zum Transatlantischen Datenschutzrahmen.
[161] Vgl. *Europäische Kommission* (Hrsg.), Trans-Antlantic Data Privacy Framework.

die Investoren basierend darauf ihre Entscheidungen fällen können. Hierzu muss das zu bewertende Risiko im ersten Schritt einen gewissen Materialisierungsgrad erreicht haben.

2.5.1 Stadien der Wesentlichkeit von ESG-Risiken

Für die Ermittlung des Risikos und des anschließenden ESG-Scores wird vorausgesetzt, dass die Risiken wesentlich sind und auch materialisiert werden können. D.h. Risiken, die sich aus der Verletzung des Datenschutzes ergeben, müssen messbar sein, um in dem Berechnungsmodell für den ESG-Score aufgenommen werden zu können. MSCI ESG Research definiert unter einem materiellen Risiko folgendes: “Ein Risiko ist für einen Wirtschaftszweig dann wesentlich, wenn es wahrscheinlich ist, dass diesen Unternehmen dadurch erhebliche Kosten entstehen (z. B. Verbot eines wichtigen chemischen Einsatzstoffs durch die Regulierungsbehörde, wodurch eine Neuformulierung erforderlich wird).“[162] Daher ist zu Beginn die Frage zu klären, ob Datenschutzrisiken eine Wesentlichkeit bergen und materiell determiniert werden können. Bis sich ein ESG relevantes Risiko jedoch materialisiert durchläuft es unterschiedliche Stadien:[163]

Erste Anzeichen lassen sich im Stadium **„Status Quo“** abzeichnen. In der ersten Stufe deviieren die Interessen der Gesellschaft von den Interessen des Unternehmens. Dieses Missverhältnis wird in der Regel nicht bewusst durch die Unternehmen erzeugt, sondern vielmehr als zwingender Nachteil für die Gesellschaft oder als verhältnismäßig unwesentlich eingestuft; im Gegensatz zu dem gesellschaftlichen Nutzen, der durch die Produkte oder Dienstleistungen entsteht.[164] Die Fehlausrichtung des Unternehmens wird aufgrund diverser Gründe durch die Gesellschaft geduldet. Gründe hierfür kann zum einen die fehlende Sensibilisierung, kollidierende moralische Normen (bspw. die kontroverse Diskussion um die Abtreibung in den USA) oder eine fehlende Mehrheit aufgrund Fehlinformationen sein.[165]

Der Status Quo ebnet den Weg für die nächste Phase, die als **„Katalysator“** bezeichnet wird. Hiermit beginnt auch der Weg der Materialisierung des Risikos. In diesem Stadium werden zwei Szenarios unterschieden: im ersten Szenario wird die Interessensabweichung durch das Unternehmen und dessen wirtschaftliche Bestreben selbst verschärft.[166] Zwar können Unternehmen durch ihr Fehlverhalten temporär exorbitante Renditen erzielen. Allerdings geraten Unternehmen hierdurch in Versuchung weitere Renditen auszuschöpfen und bspw. eine aggressivere Preispolitik zu betreiben. Das zweite Szenario tritt dann auf, wenn sich die gesellschaftlichen Ansprüche und Normen von der Tätigkeit des Unternehmens distanzieren.[167] Ursächlich hierfür sind grundsätzlich neue Informationen über die Tätigkeit des Unternehmens und/oder die tatsächlich negativen Folgen der Produkte oder Dienstleistungen.[168] Je mehr Informationen den Stakeholdern zur Verfügung

[162] *MSCI (Hrsg.),* MSCI ESG Ratings Methodology, S. 3.
[163] Vgl. *Freiberg/Rogers/Serafeim*, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 6.
[164] Vgl. *Freiberg/Rogers/Serafeim*, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 7.
[165] Vgl. *Freiberg/Rogers/Serafeim*, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 7.
[166] Vgl. *Freiberg/Rogers/Serafeim*, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 11; z.B. *Jena*, US drug prices higher than in the rest of the world, here’s why.
[167] Vgl. *Freiberg/Rogers/Serafeim*, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 11.
[168] Vgl. *Freiberg/Rogers/Serafeim*, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 12.

stehen, umso mehr kann sich dieses Missverhältnis der Interessen zuspitzen oder auch abmildern.

Dieser Umstand führt dazu, dass NGO's, Medien und weitere Stakeholder auf die Fehlausrichtung der Unternehmen reagieren, wodurch auch diese Etappe als **„Stakeholder Reaction"** bezeichnet wird.[169] Relevante Stakeholder erhöhen das öffentliche Interesse, indem sie sich entweder an die Öffentlichkeit oder an die Politik wenden und zu einem Boykott aufrufen oder eine Reform der aktuellen Gesetzeslage fordern. Erste substanzierte Anzeichen für eine Materialisierung der ESG-Risiken lassen sich dieser Phase entnehmen. Die Dynamik der Stakeholder-Reaktionen nimmt daher zu. Die Reaktion der Stakeholder erhöht überdies die Wahrscheinlichkeit weiterer Untersuchungen und Ermittlungen, regulatorischer Änderungen und einem Imageschaden. Diese Phase ist demnach insbesondere als Auslöser für eine negative oder auch positive Änderungen des Unternehmenswertes (z.B. Sturz des Aktienkurses) wahrzunehmen, die jedoch nur ein bestimmtes Unternehmen betreffen.[170] Als Antwort auf die Stakeholder reagieren Unternehmen mit Maßnahmen, die wieder das Vertrauen der Gesellschaft herstellen sollen.[171]

Damit beginnt die **„Company and Industry Reaction"** und die vierte Phase des Materialisierungsprozesses. Unternehmen sind diversen Änderungen in ihrer Unternehmenstätigkeit oder Organisation aufgrund der Erwartungshaltung der Stakeholder ausgesetzt. Als Folge daraus setzt dies für die betroffenen Unternehmen voraus, Investitionen in vertrauensbildende Maßnahmen zu tätigen und/oder führt zur Erhöhung der eigenen Kosten bspw. der Herstellungskosten. Neben der Wahrung oder Verbesserung des Unternehmensimages steht im Unternehmensfokus die Lenkung des gesellschaftlichen Diskurses und die Vermeidung regulatorischer (rigoroseren) Reformen.[172]

Gelingt dies den Unternehmen nicht, tritt das Szenario **„Regulation and Innovation"** ein. Dieses Stadium wird anhand Verabschiedungen entsprechender Regelwerke und Disruption der Märkte durch Innovation zur Forcierung einer Angleichung an die Forderungen der Gesellschaft gekennzeichnet. Die starke Dynamik, der Unternehmen unterliegen, bedingt ein volatileres Geschäftsumfeld und dadurch wesentlichere Änderungen der Aktienkurse sowie des Unternehmenswertes.[173] In Ermangelung genügender Macht seitens der Stakeholder das bestimmte ESG-Risiko zu materialisieren, bilden effektive Regularien und Gesetze eine fundamentale Grundlage zur Ermittlung des Wertes eines Risikos.[174] D.h. der Gesetzgeber erlässt Regelwerke, die entweder Bußgelder, Sanktionen oder dezidierte Maßvorgaben beinhalten und eine Materialisierung der drohenden Konsequenzen und EGS-Risiken für Unternehmen wesentlich machen.

[169] Vgl. *Freiberg/Rogers/Serafeim*, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 16 f.
[170] Vgl. *Freiberg/Rogers/Serafeim*, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 16 ff.
[171] Vgl. *Freiberg/Rogers/Serafeim*, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 21 f.
[172] Vgl. *Freiberg/Rogers/Serafeim*, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 21 f.
[173] Vgl. *Freiberg/Rogers/Serafeim*, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 24.
[174] Vgl. *Freiberg/Rogers/Serafeim*, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 24.

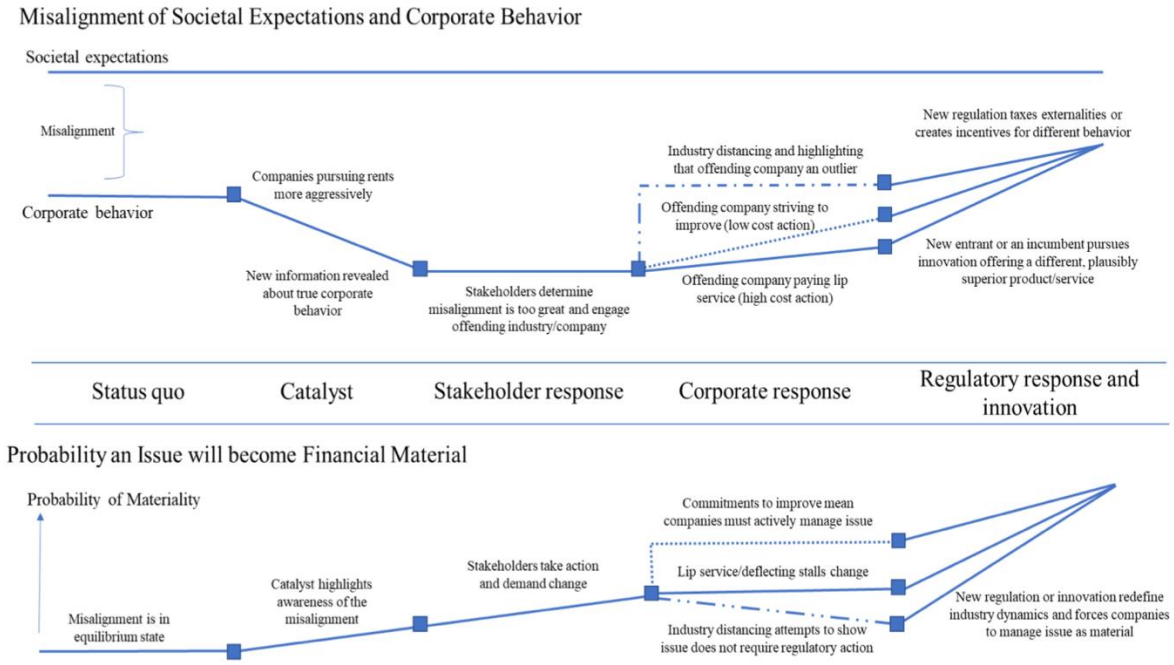

Abbildung 7: The Dynamic of Financial Materiality.

Freiberg/Rogers/Serafeim, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 28.

2.5.2 Reifegrad des Datenschutzes zur Materialisierung als ESG-Risiko

Von erheblicher Bedeutung ist es daher, dass der Datenschutz den notwendigen Reifegrad erreicht, um eine Materialisierung und damit eine Etablierung in den ESG-Score vornehmen zu können. Der Diskurs über den Umgang mit den Daten durch die Tech-Unternehmen nahm in Form von öffentlicher Berichterstattung über mehrere Jahre Gestalt. Bereits diese thematisierten den dubiosen Umgang wie etwa die Verarbeitung oder den Verkauf von Kundendaten, die folgerichtig in zahlreiche und öffentlichkeitswirksame Skandale mündeten. Der bereits oben benannte Cambridge Analytica-Fall fingiert als Repräsentant der Materialisierung des Datenschutzes (siehe Abbildung 8).[175] Die Veröffentlichung des Datenskandals entfachte einen öffentlichen Diskurs und forderte eine Stellungnahme von Mark Zuckerberg (CEO Facebook, (umbenannt in Meta)), welcher sich daraufhin in einer Kongressanhörung zu dem Vorfall äußerte.[176] Als Antwort auf die öffentliche Debatte versuchten Tech-Unternehmen, eigenverantwortlich Maßnahmen zur Erhöhung des Datenschutzes und der Datensicherheit zu ergreifen, um einer Datenschutzregulierung zuvorzukommen. Das Risiko für Unternehmen, die in den USA ansässig waren, war aufgrund der erlassenen DSGVO ohnehin bereits groß, da diese gemäß dem Marktortprinzip alle Unternehmen erfasst – unabhängig von ihrem Sitz –, die personenbezogenen Daten von Betroffenen in der Europäischen Union verarbeiten (Art. 3 Abs. 2 DSGVO). Da viele Tech-Unternehmen die Verarbeitung und den Handel mit personenbezogenen Daten als eines ihrer Kerngeschäfte definieren, hatten die Forderungen der Gesellschaft nach mehr Datenschutz eine disruptive Wirkung und zwang Unternehmen zum Umden-

[175] Vgl. *Freiberg/Rogers/Serafeim*, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 23.
[176] Vgl. *Kühl*, Facebook – Kongress 2:0.

ken ihrer Strategie.[177] Derweil lassen sich auch im US-Raum entsprechende Gesetze zur Regulierung des Umganges mit personenbezogenen Daten finden, wie etwa der California Consumer Privacy Act[178] oder jüngst der Utah Consumer Privacy Act[179]. Dies dürfte somit die Annahme rechtfertigen, dass sich Datenschutzrisiken hinsichtlich des ESG-Scores im Stadium Regulation and Innovation befinden und daher den Reifegrad zur Materialisierung erfüllen.

	Data Privacy: Facebook
Status Quo	British political consulting firm Cambridge Analytica harvested personal data from millions of Facebook profiles without knowledge or consent from users. These data were used for political advertising purposes. While some users consented to their personal information being collected through a survey, which stated was for academic use only, Facebook's design allowed personal information to be collected from non-consenting users who were in the social networks of consenting users.
Catalysts	Despite reports of illicit personal data harvesting going back to 2015 (of which Facebook was aware per Attorney General for District of Columbia)[15], the scandal went mainstream in March 2018 following emergence of an ex-Cambridge Analytica employee whistle-blowers.
Stakeholder Response	Outraged Facebook users claimed the company was consciously misusing personal data. On July 26, 2018 alone, more than $100 billion was lost from Facebook's market capitalization.
Company Response	Facebook CEO Mark Zuckerberg publicly apologized and pledged to address the issues which led to the scandal by both limiting scope of and ease of access to user personal data for developers. Facebook also announced they would voluntarily enforce the EU's General Data Protection Regulation in all areas in which Facebook operates.
Regulatory Response	Zuckerberg was called upon to testify before Congress in what became a highly publicized testimony. In 2019, the Federal Trade Commission approved fining Facebook $5 billion following an investigation of the scandal. While no major federal regulation has been enacted in the US, in June 2018 California passed the California Consumer Privacy Act which stipulates greater data protection for consumers.

Abbildung 8: Materiality Development in Four Industries – Data Privacy.

Freiberg/Rogers/Serafeim, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 14.

[177] Vgl. *Freiberg/Rogers/Serafeim*, How ESG Issues Become Financially Material to Corporations and Their Investors, S. 23.
[178] Vgl. California Consumer Privacy Act of 2018 [1798.100 - 1798.199].
[179] Vgl. Consumer Privacy Act 2022, General State of Utah vom 25.2.2022.

2.5.3 Beschreibung und Funktionsweise des ESG-Scores

Die Bewertung von Unternehmen mittels eines ESG-Scores stellt einen elementaren Bestandteil zur Messung und Umsetzung von gesellschaftlichen und gesetzlichen Anforderungen dar. Auf diese Weise ist es möglich, ein Unternehmen und dessen Geschäftspraktiken im Hinblick auf die drei ESG-Risiken zu evaluieren. Für Investoren ergibt sich hierdurch die Möglichkeit, Unternehmensbenchmarks und Investitionsentscheidungen basierend auf den eigenen Präferenzen zu treffen. ESG-Ratings beschreiben dabei einen Bewertungsrahmen, mit dem die Leistung eines börsennotierten oder in Privatbesitz befindlichen Unternehmens, Sektors oder Landes in Bezug auf ESG-Faktoren systematisch bewertet und gemessen wird, um einen kombinierten ESG-Score für dieses Unternehmen, diesen Sektor oder dieses Land zu ermitteln. ESG-Scores stellen dabei ein zentrales Werkzeug für Investoren dar, die die Leistung ihres ESG-Portfolios zusätzlich oder anstelle ihres konventionellen Benchmarks verfolgen wollen. ESG-Ratings sind vielfältig einsetzbar und können alle Unternehmensgrößen oder Institutionen umfassen sowie unterschiedliche Assets wie z.B. von öffentliche Aktien bis zu Immobilien, die Infrastruktur oder Staatsanleihen bewerten. Der ESG-Score stellt einen nach Marktkapitalisierung gewichteten Wert dar, der durch die Aggregation der Unternehmensbewertungen auf Grundlage der ESG-Risiken berechnet wird.[180] Mithilfe des ESG-Scores wird der Investmentmarkt in die Lage versetzt, die Auswirkungen von ESG-Strategien auf Portfolios zu messen, die finanziellen Auswirkungen von ESG-Strategien zu quantifizieren, die ESG-Merkmale von Portfolios zu definieren und/oder das ESG-Risiko zu ermitteln.[181] Dabei hält der Markt zahlreiche Agenturen bereit, die die Unternehmen hinsichtlich den drei ESG-Kriterien bewerten und evaluieren. Die Ratingagenturen stellen dabei auf ein nicht harmonisiertes Bewertungsverfahren nach individuellen Berechnungsmethoden und Kriterien ab.[182] Da es hier eine Bandbreite an Ratingagenturen gibt, beschränkt sich das folgende Kapitel auf die Berechnungsmethode des Marktführers MSCI in ESG Ratings und wie sich eine gerechte Berücksichtigung des Datenschutzes im Rahmen dessen ausgestalten ließe.

2.5.3.1 MSCI ESG Rating – Methodik und Berechnung des ESG-Ratings

MSCI ESG Rating ist eine Ratingagentur mit Hauptsitz in New York, die mit über 1.500 verschiedenen ESG-Indizes und 130 Analysten der weltweit größte Anbieter in diesem Bereich ist.[183] Hierzu analysieren diese Daten aus öffentlichen Informationen und Dokumenten (wie bspw. 10-K, Nachhaltigkeitsberichten und Stimmrechtsvollmachten) sowie über 1000 spezialisierte Datensätze (der Regierung, NGO und Eigentumsmodelle). Ein wichtiges Instrument sind dabei globale und lokale Medienpublikationen, wovon MSCI ESG Research täglich mehr als 1600 überwacht.[184]

[180] Vgl. *Pagano/Sinclair/Yang*, in: Research handbook of finance and sustainability, S. 341.
[181] Vgl. *Pagano/Sinclair/Yang*, in: Research handbook of finance and sustainability, S. 342.
[182] Vgl. *Sahin/Bax/Czado/Paterlini*, Environmental, Social, Governance scores and the missing pillar – Why does missing information matter?, S. 3.
[183] Vgl.*Greiten*, Übersicht über die wichtigsten ESG-Ratings – und was sie für die Finanzkommunikation bedeuten.
[184] Vgl.*Pagano/Sinclair/Yang*, in: Research handbook of finance and sustainability, S. 349.

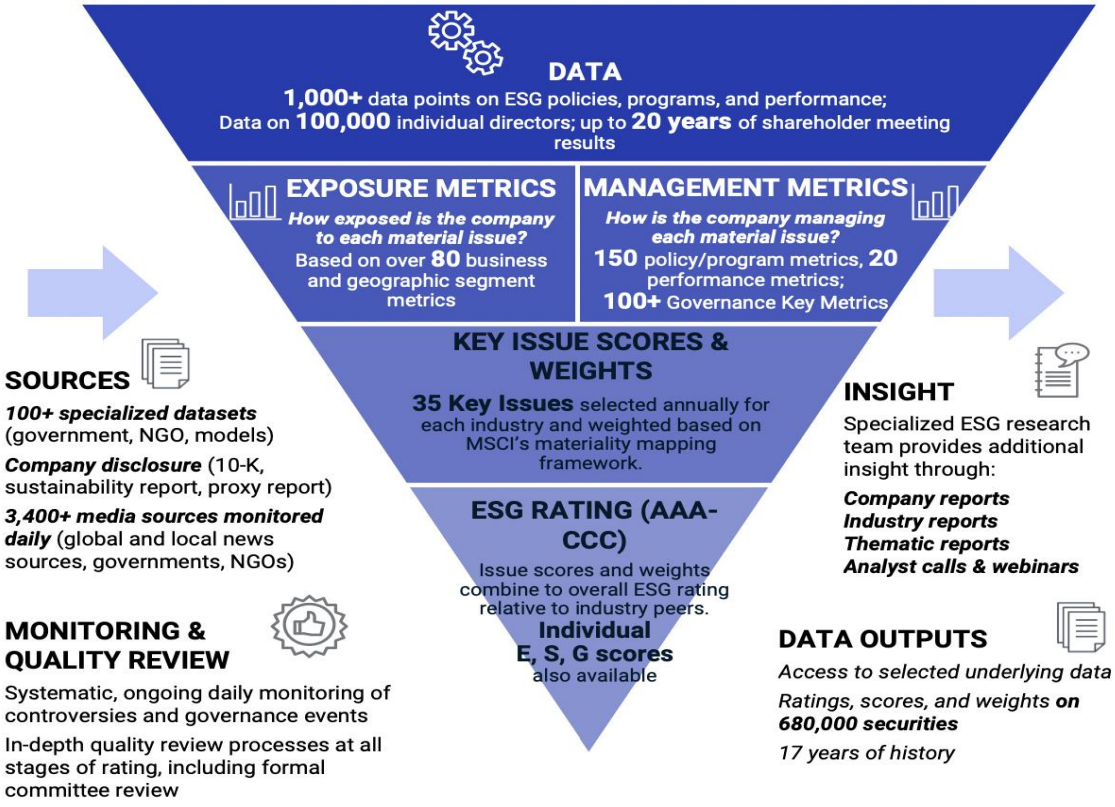

Abbildung 9: ESG Rating Framework and Process Overview.

MSCI (Hrsg.), MSCI ESG Ratings Methodology, S. 2.

Ziel des MSCI ESG Ratings ist es, die Resilienz eines Unternehmens hinsichtlich der ESG-Risiken zu messen. Hierzu untersucht MSCI ESG Rating das Unternehmen auf die folgenden vier Fragen[185]:

1. Welche Kernrisiken und Chancen im Bereich ESG bestehen für das Unternehmen und dessen Sektor?
2. Wie stark ist das Unternehmen den Risiken und/oder Chancen ausgesetzt?
3. Wie sieht das Risikomanagement des Unternehmens aus?
4. Wie sieht das Gesamtbild des Unternehmens aus und wie steht es im Vergleich zu seinen Wettbewerbern dar?

2.5.3.1.1 1. Schritt: Ermittlung des Key Issue Scores für die betroffene Industrie im Bereich Environment und Social

Im ersten Schritt werden die Kernrisiken (Key Issue Score) für die entsprechende Industrie aus der Global Industry Classification Standards (im Folgenden „GICS“)[186] erfasst. In dieser Phase der Bewertung können anhand allgemeiner Informationen die Datenschutzrisiken für die betreffende Industrie ermittelt werden. Das GSCI unterscheidet hierbei zwi-

[185] Vgl. *MSCI (Hrsg.),* MSCI ESG Ratings Methodology, S. 3.

[186] Der GCSI wurde von MSCI in Kooperation mit Standard & Poor's entwickelt und klassifiziert Unternehmen in 11 Sektoren, welcher wiederum Kategorien wie Industriegruppen, Industrien und Subindustrien beinhaltet; *MSCI (Hrsg.),* The Global Industry Classification Standard; vgl. *MSCI (Hrsg.)*, What You Need to Know About MSCI ESG, S. 24.

schen 11 Sektoren, die sich je nach ihrer Geschäftstätigkeit hinsichtlich ihrer Risiken unterscheiden.[187] Eine analoge Anwendung dürfte auch bei der Ermittlung von Datenschutzrisiken sinnvoll sein, da diese je nach Branche/Sektor/angebotene Produkte variieren. So dürfte der Gesundheitssektor grundsätzlich größeren Datenschutzrisiken aufgrund der größeren Menge an besonderen personenbezogenen Daten ausgesetzt sein als bspw. der Energiesektor.[188] Art. 83 lit. g) DSGVO sieht für Verstöße, die besondere Kategorien personenbezogener Daten betreffen, die Aussprache erhöhter Bußgelder an.[189] So sprach die französische Datenschutz-Aufsichtsbehörde CNIL an das Software-Unternehmen Deadulus Biologie eine Bußgeldzahlung i.H.v. 1,5 Millionen Euro aus, da aufgrund einer Sicherheitslücke Gesundheitsdaten von 500.000 Betroffenen im Internet veröffentlicht wurden.[190] Daraufhin werden die Risiken im Bereich Environment und Social nach einem festen Schema gewichtet (Key Issue Weights) (siehe Abbildung 10). Jedes Environmental- oder Social-Risiko wird mit 5% - 30% im Rahmen des gesamten Ratings gewichtet. In der Gewichtung werden die Maßnahmen der Industrie in Relation zu anderen Industrien hinsichtlich der negativen und positiven Auswirkungen auf die Gesellschaft und das Zeitfenster, in dem sich das Risiko materialisiert, berücksichtigt.[191] Hierbei könnten die Maßnahmen des Unternehmens im Bereich des Datenschutzes in der Bewertung des Key Issue Scores wiederfinden.

		Expected Time frame for Risk/Opportunity to Materialize	
		Short-Term (<2 years)	**Long-Term** (5+ years)
Level of Contribution to Environmental or Social Impact	Industry is **major** contributor to impact	**Highest Weight**	
	Industry is **minor** contributor to impact		**Lowest Weight**

Abbildung 10: Framework for setting Key Issue Weights.

MSCI (Hrsg.), MSCI ESG Ratings Methodology, S. 5.

Risiken mit „Highest Weight“ und „Short-Term“ werden mit drei multipliziert und damit mehr gewichtet als Risiken, die „Lowest Weight“ und „Long Term“ aufweisen.[192] Governance-Risiken hingegen werden für alle GICS-Subindustrien entweder mit „High Impact/Long Term“ und „Medium Impact/Long Term“ angenommen. Die Gewichtung der Governance-Säule wird mit mindestens 33% angesetzt und umfasst die Bewertung der Corporate Governance und Corporate Behaviour.[193]

[187] Vgl. *MSCI (Hrsg.)* The Global Industry Classification Standard.
[188] Vgl. *Giese/Nagy/Lee*, Welche ESG-Kriterien waren die wichtigsten? Definition von Ereignis- und Erosionsrisiken.
[189] In Art. 83 Abs. 2 lit. g) DSGVO stellt der Gesetzgeber auf die Kategorie der verarbeitenden Daten ab.
[190] Vgl.*Activemind.AG (Hrsg.)*, 1,5 Mio. Euro Bußgeld wegen massiven Lecks bei Gesundheitsdaten.
[191] Vgl .*MSCI (Hrsg.),* MSCI ESG Ratings Methodology, S. 5; Vgl. *MSCI (Hrsg.)*, What You Need to Know About MSCI ESG, S. 25.
[192] Vgl. *MSCI (Hrsg.),* MSCI ESG Ratings Methodology, S. 5.
[193] Vgl. *MSCI (Hrsg.),* MSCI ESG Ratings Methodology, S. 6.

2.5.3.1.2 2. Schritt: Evaluierung des individuellen Risikoprofils (Key Issue Assessment)

Um den individuellen Score eines dezidierten Unternehmens zu ermitteln, werden das Kerngeschäft, die Produkte oder Dienstleistungen, die Niederlassung der Produktion und weitere relevante Faktoren wie etwa die Auslagerung von bestimmten Geschäftsbereichen berücksichtigt.[194] Hierbei bewertet MSCI ESG Rating zum einen das individuelle Risiko des Unternehmens („Risk Exposure Score") und die Maßnahmen im Rahmen des Risikomanagements („Risk Management Score"), die zur Risikominimierung eingesetzt werden. Z.B. erhöht sich das Risiko einer Investition in ein Unternehmen, insofern dieses seinen Sitz in einem unsicheren Drittland[195] hat. Angesichts der Niederlassung des Technologieunternehmens Meta in den USA[196], der großen Datenmenge sowie der Vielzahl an hohen Bußgeldern[197] dürfte die Investition in Meta hinsichtlich der Datenschutzaspekte mit größeren Risiken verbunden sein als ein Technologieunternehmen mit Sitz innerhalb der Europäischen Union. Selbiges gilt auch für Unternehmen, deren Kerngeschäft die Verarbeitung von personenbezogenen Daten zum Gegenstand hat und somit das Kundenverhalten trackt, um sodann ein Kundenprofil zu erstellen sowie Werbeanzeigen zu optimieren, wie bspw. Trackingtools.

Beide Kriterien werden auf einer Skala von 0-10 repräsentiert. Während ein Risk Exposure Score von 0 kein Risiko darstellt, ist das Unternehmen bei einem Score von 10 am stärksten den Kernrisiken ausgesetzt. Ein Management Score von 0 gibt keine Managementbemühungen wieder; über ein sehr gutes Management verfügt das Unternehmen jedoch bei einem Management Score von 10.[198] Im Ergebnis werden beide Kennzahlen ins Verhältnis gesetzt, sodass ein höheres Risiko des Unternehmens ein anspruchsvolleres Risikomanagement voraussetzt. Auf diese Weise wird für die gesamte Industrie derselbe Key Issue Score erzielt.

Die Opportunitäten für das jeweilige Unternehmen werden anhand des gleichen Bewertungsverfahrens evaluiert. Jedoch mit dem Unterschied, dass zum einen der Opportunity Exposure Score und zum anderen die Fähigkeit des Unternehmens von dieser Möglichkeit zu profitieren in Betracht gezogen wird.

2.5.3.1.3 3. Schritt: Ermittlung des Governance-Scores

Während der Berechnungsansatz des Environmental- und Social-Scores individuelle Faktoren erfasst, verfolgt die Ermittlung des Governance-Scores einen absoluten Ansatz, der auf einer allgemeingültigen Skala von 0-10 beruht. Dem liegen sowohl der Themen-Score

---

[194] Vgl. *MSCI (Hrsg.),* MSCI ESG Ratings Methodology, S. 7.

[195] „Sichere Drittländer" sind solche, denen die Europäische Kommission per Angemessenheitsbeschlusses ein angemessenes Datenschutzniveau bestätigt hat. Dort gewährleisten die nationalen Gesetze einen Schutz von personenbezogenen Daten, welcher mit dem des EU-Rechts vergleichbar ist. Zu den sicheren Drittstaaten gehören: Andorra, Argentinien, Kanada (nur kommerzielle Organisationen), Färöer, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Schweiz, Uruguay, Japan, das Vereinigte Königreich und Südkorea. In diese ist die Datenübermittlung daher ausdrücklich gestattet.

[196] Mit dem Urteil „Schrems II" vom 16. Juli 2020 (Az.: C-311/18) hat der EuGH den Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild (Privacy Shield) gebotenen Schutzes mit sofortiger Wirkung für ungültig erklärt. Datenübermittlungen in die USA können folglich nicht auf das Privacy Shield gestützt werden. Datentransfers in die USA bedürfen anderer Garantien, i. S. v. Art. 44 ff. DSGVO, zur Herstellung eines angemessenen Datenschutzniveaus.

[197] Vgl. *CNIL (Hrsg.),* Cookies: FACEBOOK IRELAND LIMITED fined 60 million euros; *ZEIT ONLINE (Hrsg.)*, WhatsApp muss Strafe von 225 Millionen Euro zahlen.

[198] Vgl. *MSCI (Hrsg.),* MSCI ESG Ratings Methodology, S. 7.

als auch der Key-Issue-Score zugrunde (siehe Abbildung 11). Diese werden unabhängig voneinander berechnet und von dem maximalen Score von 10 Punkten abgezogen, je nachdem, welcher Score bei den zugrundeliegenden Key-Issues berechnet werden.[199] Der elementare Unterschied zur Berechnung unter Schritt 1 ist, dass die Gewichtung erst auf der Säulen-Ebene statt auf der Key-Issue-Ebene vorgenommen wird.[200]

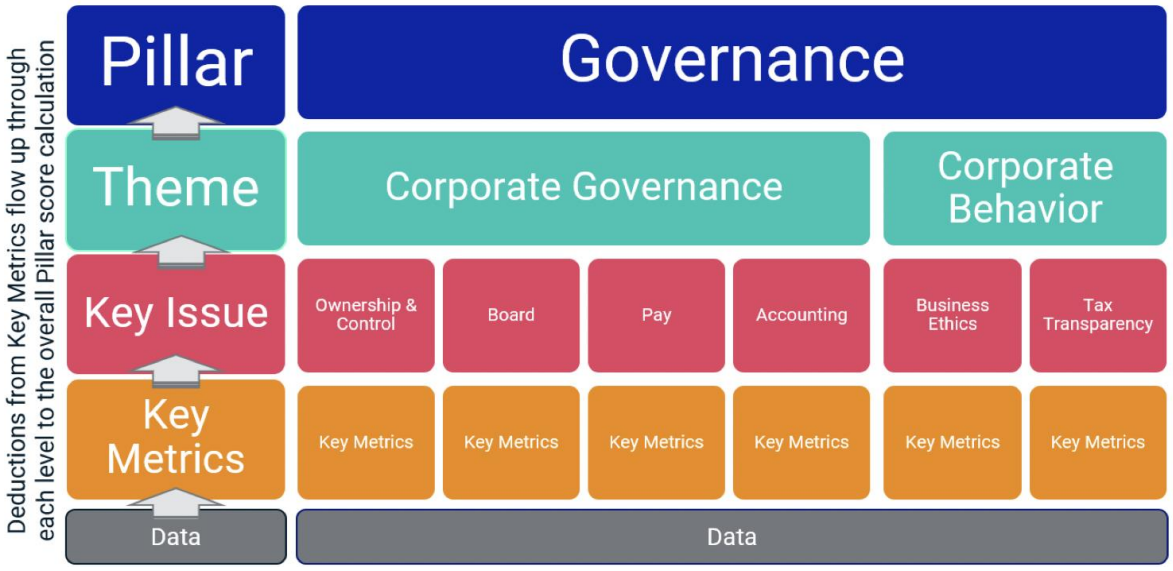

Abbildung 11: Governance Model Structure.

MSCI (Hrsg.), MSCI ESG Ratings Methodology, S. 10.

2.5.3.1.4 4. Schritt: Die Berechnung des endgültigen ESG-Scores

Um den endgültigen und bereinigten ESG-Score zu ermitteln, wird der gewichtete Durchschnitt der einzelnen Säulen Environment und Social (Key Issue Weights) und jener der Governance-Säule herangezogen. Dadurch erhält jedes Unternehmen den sog. Industry-Adjusted Score (IAS), der auf den festgelegten Marktwerten basiert. Nach Berücksichtigung etwaiger Überschreitungen auf Ausschussebene entspricht die endgültige branchenangepasste Punktzahl jedes Unternehmens einer Bewertung zwischen der besten (AAA) und der schlechtesten (CCC). Diese Bewertungen sind nicht absolut, sondern sollen ausdrücklich relativ zu den Wettbewerbern eines Unternehmens verstanden werden.[201]

[199] *MSCI (Hrsg.),* MSCI ESG Ratings Methodology, S. 10.
[200] *MSCI (Hrsg.),* MSCI ESG Ratings Methodology, S. 11.
[201] *MSCI (Hrsg.),* MSCI ESG Ratings Methodology, S. 11.

Letter Rating	Leader/Laggard	Final Industry-Adjusted Company Score
AAA	Leader	8.571* - 10.0
AA	Leader	7.143 – 8.571
A	Average	5.714 – 7.143
BBB	Average	4.286 – 5.714
BB	Average	2.857 – 4.286
B	Laggard	1.429 – 2.857
CCC	Laggard	0.0 – 1.429

Abbildung 12: Mapping the Industry Adjusted Company Score to Letter Ratings.

MSCI (Hrsg.), MSCI ESG Ratings Methodology, S. 12.

2.5.4 Kritik an der bisherigen Einbindung des Datenschutzes in das ESG-Rating

Das Berechnungsmodell weist diverse Defizite auf, die einer adäquaten Einbindung des Datenschutzes nicht zufriedenstellend Rechnung tragen. Als Konsequenz hieraus können die Folgen einer Missachtung der DSGVO nicht dem Umstand entsprechend gewichtet und fälschlicherweise nicht als Key Issue für die betroffene Industrie identifiziert werden. Hierdurch entsteht nicht nur eine „Scheintransparenz“ für die Anleger und Investoren, sondern kann vielmehr für das Datenschutzrisikomanagement der Unternehmen folgenschwere Konsequenzen haben. Jene Unternehmen stützen sich auf falsch oder besser bewertete ESG-Scorings, die diese zu keinen weiteren Optimierungsmaßnahmen des eigenen Datenschutzmanagementsystems anreizen. Ferner wird durch eine solche Informationsasymmetrie das primäre Ziel des ESG-Ansatzes – eine transparente Informationsgrundlage zur Festlegung von nachhaltigen Investitionsentscheidungen – verfehlt. Eine nicht angemessene Informationsgrundlage führt folglich auch zu einer Fehleinschätzung des Risikos und zu Fehlentscheidungen. Anlässlich dessen ist die Berücksichtigung des Datenschutzes in dem MSCI ESG Rating kritisch zu beäugen.

2.5.4.1 Kategorisierung des Datenschutzes in die Produkthaftung

Wie der Abbildung 13 entnommen werden kann, ordnet MSCI den Datenschutz fälschlicherweise ´dem Themengebiet Produkthaftung zu, wodurch die Bedeutung des Datenschutzes für Unternehmen und die damit verbundenen Risiken nicht ausreichend zum Tragen kommen.

Abbildung 13: MSCI ESG Rating Model, Key Issues.

MSCI (Hrsg.), MSCI ESG Ratings Methodology, S. 18.

Sowohl der weite Betroffenenkreis nach Art. 4 Nr. 1 DSGVO als auch die Anwendung der DSGVO auf alle Verarbeitungsvorgänge lässt herleiten, dass diese nicht ausschließlich auf die vom Verantwortlichen hergestellten Produkte beschränkt ist, wodurch die Zuordnung zur Produkthaftung durch das MSCI nicht sachgemäß erscheint. Maßgeblich für die Produkthaftung innerhalb Deutschlands ist das Produkthaftungsgesetz (im Folgenden ProdHaftG)[202], welches der Umsetzung der Europäischen Produkthaftungsrichtlinie[203] dient. Die Produkthaftung bezieht sich ausschließlich auf die Haftung des Herstellers und die kohärenten Schadensersatzzahlungen, wenn durch einen Produktfehler jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt wird, § 1 ProdHaftG. Ein Produkt ist dabei gem. § 2 ProdHaftG jede bewegliche Sache, auch wenn sie einen Teil einer anderen beweglichen Sache oder einer unbeweglichen Sache bildet, sowie Elektrizität. Die Produkthaftungsrichtlinie konkretisiert dies in einem Erwägungsgrund und umfasst ausdrücklich physische Schäden: „Damit der Verbraucher in seiner **körperlichen Unversehrtheit und seinem Eigentum** geschützt wird …“, „Der Schutz des Verbrauchers erfordert die Wiedergutmachung von Schäden, die **durch Tod und Körperverletzungen verursacht wurden**, sowie die Wiedergutmachung von Sachschäden“. Schadensersatzansprüche aufgrund nicht datenschutzkonformer Produkte, die zu einer Verletzung der körperlichen Unversehrtheit führen oder gar das Eigentum beschädigen scheinen jedoch eher unwahrscheinlich, wodurch die Anwendung der Produkthaftung an der Stelle obsolet sein dürfte.[204] Zumal bereits die Anwendbarkeit der Produkthaftung wie z.B. bei einer Software aufgrund mangels Erfüllung der Definition eines Produkts in Frage zu stellen ist.[205] Die Tatsache, dass sich aus der deliktischen Produzentenhaftung nach § 823 Abs. 1 BGB eine Pflicht zur Herstellung

[202] Gesetz über die Haftung für fehlerhafte Produkte vom 15. Dezember 1989, im Folgenden: Produkthaftungsgesetz.

[203] Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte, im Folgenden: Produkthaftungsrichtlinie.

[204] Die Gerichtspraxis befasst sich überwiegend mit der Frage des immateriellen Schadensersatzanspruchs, vgl., *Leibold*, ZD 2022, 18, 38.

[205] Vgl. *Bartsch/Roth*, Zivil- und strafrechtliche Möglichkeiten zur Durchsetzung der gesetzlichen Vorgaben zum Datenschutz am Beispiel arbeitsteiliger Verarbeitungsvorgänge im nicht-öffentlichen Bereich, EnWZ 2018, 435 ff.; *Reusch*, BB 2019, 904, 905 f.

datenschutzkonformer Produkte begründen ließe[206] sei indes dahingestellt, da der Anspruch lex specialis neben dem Schadensersatzanspruch aus Art. 82 DSGVO steht. Zwar mögen der Datenschutz und die Datensicherheit in der Entwicklungsphase von den Produkten auch eine tragende Rolle spielen, so bspw. die beiden Grundsätze Datenschutz durch Technikgestaltung (Privacy by Design) und datenschutzrechtliche Voreinstellung (Privacy by Default). Hierdurch müssen bereits zum Zeitpunkt der **Planung eines Verarbeitungssystems** technische und organisatorische Maßnahmen getroffen werden, um insbesondere die Sicherheit der Daten zu gewährleisten, ErwGr. 78 DSGVO.[207] Jedoch beziehen sich der Datenschutz und die Datensicherheit weder ausschließlich auf Produkte i.S.d. des § 2 ProdHaftG noch lassen sich weitere Parallelen oder Schnittmengen zur Produkthaftung finden, die eine Unterkategorisierung begründen ließen. Zum einen würde eine Einordnung des Datenschutzes in die Kategorie Produkthaftung das Ziel des Rechts auf informationelle Selbstbestimmung in anderen Sektoren, die keine Produkte im herkömmlichen Sinne herstellen oder in Verkehr bringen wie bspw. Dienstleister, nicht effektiv umsetzen oder gar verfehlen. Die DSGVO erwähnt ferner explizit, dass der Datenschutz bei jedem Verarbeitungsvorgang (-system), der die Verarbeitung von personenbezogenen Daten zum Gegenstad hat – unabhängig davon, ob es sich um einen Herstellungsprozess des Produktes handelt –, zu beachten ist (ErwGr. 2). Zum anderen verfolgt die Produkthaftung primär das Ziel, die physische Gesundheit und Sicherheit der Verbraucher zu gewährleisten.[208] Das Recht auf Datenschutz hingegen ist ein Persönlichkeitsrecht, das natürliche Personen insbesondere vor Gefahren der automatisierten Datenverarbeitung schützen soll.[209] Die Datensicherheit zielt darauf ab, die Daten vor Verlust, Verfälschung und unberechtigtem Zugriff zu schützen.[210] Diese sollen insbesondere die zunehmende Digitalisierung im Zuge von Big Data und künstlicher Intelligenz im Interesse und in Konformität mit den Grundrechten der Verbraucher sowie betroffenen Personen bringen[211] und haben daher wenig gemein mit der physischen Gesundheit im Sinne der Produkthaftung. Anlässlich dessen dürfte es sinnvoll sein, eine neue Kategorie zu definieren, die nicht ausschließlich die Produkte hinsichtlich des Datenschutzes und der Datensicherheit isoliert bewertet, sondern die beiden Materien holistisch betrachtet und evaluiert. Im Lichte der exorbitant steigenden Digitalisierung biete sich der Ansatz an, die Kategorie „Digital Responsibility“ zu integrieren, sodass auch Datenschutzrisiken ermittelt werden, die nicht im unmittelbaren Zusammenhang mit der Herstellung oder dem Inverkehrbringen von Produkten stehen. Dieser Kategorie sind dann Risiken aus den Bereichen Datenschutz, Datensicherheit, Informationssicherheit und Cyber Security der Bewertung zu unterziehen. Nur auf diese Weise ist es möglich, den Datenschutz aus allen Perspektiven adäquat zu betrachten und auch Risiken zu erfassen, die bspw. vom Digitalisierungsgrad oder von der Sensibilität der Verarbeitungsvorgänge abhängig sind.

2.5.4.2 Beschränkter Fokus auf den Kundendatenschutz

Bedingt durch die Einordnung in die Subgruppe der Produkthaftung und die beschränkte Berücksichtigung des Kunden als Verbraucher der Produkte, lässt dies Grund zur Annahme, dass ausschließlich Risiken betrachtet werden, die sich im Zusammenhang mit dem Kun-

[206] Vgl. *Specht-Riemenschneider*, Herstellerhaftung für nicht-datenschutzkonform nutzbare Produkte – Und er haftet doch!, MMR 2020, 73,75.
[207] Vgl. *Intersoft Consulting (Hrsg.)*, DSGVO Privacy by Design.
[208] Vgl. Erwägungsgründe der Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte, im Folgenden. Produkthaftungsrichtlinie; ErwGr. 4 der Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit.
[209] Vgl. *Berliner Beauftragte für Datenschutz und Informationsfreiheit (Hrsg.)*, Datenschutz – Rechtliche Grundlagen.
[210] Vgl. *Gabriel/Lux/Menke*, Basiswissen Wirtschaftsinformatik, S. 306.
[211] Vgl. *Bundesministerium für Arbeit und Soziales (Hrsg.)*, Corporate Digital Responsibility.

dendatenschutz ergeben. Der Gesetzgeber erwähnt jedoch im ErwGr. 1 der DSGVO explizit, dass jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat. Zwar mögen wertschöpfende Prozesse die Mehrheit der Verarbeitungsvorgänge i.S.d. Art. 4 Nr. 2 DSGVO darstellen, wodurch der Schutz personenbezogener Daten von Kunden eine wesentliche Rolle spielt, allerdings beschränkt sich die DSGVO nicht ausschließlich auf den Kundendatenschutz. Vielmehr findet der Datenschutz auch in der Lieferantenkette Anwendung (siehe oben), in diesem Zusammenhang birgt jedoch insbesondere der Beschäftigtendatenschutz erhebliche Risiken für die Unternehmen. Dies verdeutlicht das Beispiel des Bußgeldes, das an das Textilhandelsunternehmen H&M Hennes & Mauritz Online Shop A.B. & Co. KG verhängt wurde. Das Textilhandelsunternehmen hatte Informationen bezüglich der Lebensumstände der Mitarbeiter verarbeitet und gesammelt, um Persönlichkeitsprofile zu erstellen und die Leistung der Mitarbeiter zu überwachen, woraufhin der Hamburgische Beauftragte für Datenschutz und Informationssicherheit diesem ein Bußgeld i.H.v. 35 Millionen Euro auferlegte.[212] Auch haben die Entscheidungen der Arbeitsgerichte im Bereich des Beschäftigtendatenschutzes seit der Anwendung der DSGVO stark zugenommen.[213] Die Verbreitung eines Bildes, das im Zusammenhang mit der Hautfarbe der Betroffenen steht und zur Werbung der Internationalität des Arbeitgebers ohne Einverständnis der Beschäftigten verwendet wird, wurde durch das ArbG Münster mit einem Schadensersatz von 5.000 Euro beziffert.[214]

Im Übrigen ist der Umstand nicht zu verkennen, dass während solcher Dauerschuldverhältnisse wie dem Arbeitsverhältnis eine exorbitante Menge an personenbezogenen Daten und besondere Kategorien personenbezogener Daten verarbeitet werden. Beispiele für personalbezogene Prozesse können dabei die Führung der Personalakte, die Nutzung eines Human-Capital-Managements-Systems oder die Videoüberwachung sein.[215] Andererseits machen insbesondere Beschäftigte von den Betroffenenrechten nach Art. 17 DSGVO Gebrauch, da diese auch meistens als Pendant zum Machtgefälle zwischen Arbeitgeber und Arbeitnehmer gelten.[216] Besonders Auskunftsansprüche fingieren als Katalysator datenschutzrechtlicher Verstöße und können damit eine Kettenreaktion weiterer Interventionsrechte oder gar Ermittlungen der Datenschutzbehörden auslösen. Auch das Eindringen neuer Anbieter zur Durchsetzung von Schadensersatzansprüchen oder innovativer Legal-Tech-Anwendungen auf dem Markt lassen prognostizieren, dass Datenschutzverstöße künftig an hoher medialer Präsenz genießen könnten. Zumal für das Akquirieren potenzieller Kläger und zur erfolgreichen Durchsetzung von Massenklagen, öffentlichkeitswirksame Werbung betrieben wird. Nebst Verbraucher als potenzielle Kläger können auch andere Stakeholder wie Beschäftigte oder nur Besucher einer Webseite in Frage kommen.[217]

---

[212] Vgl. *Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit (Hrsg.)*, 35,3 Millionen Euro Bußgeld wegen Datenschutzverstößen im Servicecenter von H&M.

[213] Vgl. *Böhm/Brams*, NZA-RR 2021, 521, 521.

[214] Vgl. ArbG Münster, Urteil vom 25.03.2021 – 3 Ca 391/20, ZD 2021, 534, 534.

[215] *Der Hessische Beauftragte für Datenschutz und Informationsfreiheit*, 47. Tätigkeitsbericht vom 31.12.2018, S. 80.

[216] Vgl. *Böhm/Brams,* NZA-RR 2021, 521, 521 ff; u.a. ArbG Bonn, Urteil vom 16.7.2020 – 3 Ca 2026/19, ZD 2021, 111, 111 ff; BAG, Urteil vom 27.4.2021 – 2 AZR 342/20, NJW 2021, 2379, 2379 ff.

[217] Vgl. etwa die Presseberichte unter: https://eugd.org/schadenersatz/scalable-capital/; *Handelsblatt (Hrsg.)*, Nach Datenleck: Scalable Capital soll Schadenersatz zahlen; *FAZ (Hrsg.)*, Scalable Capital soll wegen Datendiebstahl zahlen.

3 Entwicklung einer Datenschutz-Strategie im Lichte der ESG-Strategie durch die Beratung

Die bisher genannten Ausführungen unterstreichen die Notwendigkeit einer ESG-Strategie. Es ist jedoch auch unumstritten, dass jedes Unternehmen vor unterschiedlichen Herausforderungen steht; denn das Risikoprofil des Unternehmens korreliert unter anderem mit dem Sektor, dem Unternehmenssitz und der Unternehmensgröße. Nach diesen Kriterien bestimmen sich auch die Anforderungen des Marktes, wonach die Unternehmen zu agieren haben, um nachhaltig rentabel zu sein. Da diese Faktoren mit einer großen Komplexität behaftet sind, wird eine ESG-Strategie grundlegend vorausgesetzt, die unter anderem ESG-Ziele und -ambitionen beinhaltet. Dies ist umso wichtiger, da die ESG-Performance eines Unternehmens einen unmittelbaren Einfluss auf den Zugang zu Kapital, die Kostenstrukturen und die Absatzmenge haben kann. ESG sollte daher als ein zentrales Element jeder Unternehmensstrategie betrachtet werden. Jedoch müssen ESG-Risiken auch in die Geschäftsmodelle und Strategien der Unternehmen etabliert werden. Grundsätzlich ist unter einer Strategie folgendes zu verstehen:

„Eine Strategie bezeichnet – nach betriebswirtschaftlichem Verständnis – das Rahmenkonzept oder einen Leitfaden für die langfristige Erreichung von unternehmerischen Absichten und Zielen. Eine Strategie gibt zunächst nur eine allgemeine Richtung der (Unternehmens-) Entwicklung vor. Sie muss deshalb durch nachfolgende Maßnahmen konkretisiert werden. Gleichzeitig erfordert eine Strategie eine ständige Anpassung an veränderte Rahmenbedingungen“.[218] Strategien verfolgen das primäre Ziel, die Marktposition des Unternehmens nachhaltig und systematisch zu verbessern.[219]

Bedeutsam scheint in diesem Zusammenhang jedoch auch, dass in bereits bestehende oder noch zu entwickelnde ESG-Strategien simultan eine Datenschutz-Strategie zu definieren ist. Denn wie bereits oben beschrieben, können aus den Maßnahmen der anderen ESG-Dimensionen ein Spannungsverhältnis aufgrund der Kollisionen mit dem Datenschutz entstehen. Für den nachhaltigen und ethischen Umgang mit Daten (Stichwort: Corporate Digital Responsibility) ist es für Unternehmen und deren Mitarbeiter notwendig feste Handlungsvorgaben in Form einer Datenschutz-Strategie innezuhaben. Vor diesem Hintergrund ist es von großer Bedeutung, einen harmonisierten und standardisierten Prozess zu etablieren, der bei jeglichen ESG-Maßnahmen die datenschutzspezifischen Aspekte im Vorfeld beachtet. In Art. 25 DSGVO i.V.m. ErwGr. 78 findet sich zwar die Pflicht des Verantwortlichen wieder, für die von ihm geplanten Datenverarbeitung eine ausreichende Strategie unter Berücksichtigung der von der DSGVO geforderten Anforderungen vorzuhalten. Diese Strategie ist wiederum Prüfungsgegenstand des betrieblichen Datenschutzbeauftragten. Eine Datenschutz-Strategie enthält dabei vor allem Leitlinien, Bekenntnisse und eine grundsätzliche Richtungsvorgabe sowie die Bedeutung von Datenschutz im Geschäftsmodell des Unternehmens.[220] Allerdings richtet diese ihren Fokus auf die Einhaltung der beiden Grundsätze Privacy by Design und by Default. Eine Pflicht zur Etablierung einer holistischen Datenschutz-Strategie ist jedoch nicht explizit vorgesehen. Jedoch hat eine solche Strategie nicht nur vor dem Hintergrund des gesetzlich Geforderten stattzufinden, vielmehr ist sie aus der Selbstverpflichtung zum nachhaltigen Umgang

[218] *Deutsches Institut für Deutsche Revision e.V. (Hrsg.)*, Checkliste zur Prüfung der Datenschutzorganisation, S. 4.
[219] Vgl. *Haake/Rusch/Seiler/Seliner*, Strategie-Workshop, S. 13.
[220] *Deloitte (Hrsg.)*, Datenschutz-Organisation.

mit Daten in Anbetracht der steigenden Digitalisierung (Corporate Digital Responsibility) und der Anforderung des Marktes heraus, zu definieren. So ergab die Umfrage von McKinsey, dass fast 90 Prozent der Befragten auf andere Unternehmen ausweichen würden, wenn sie Bedenken hinsichtlich des Datenschutzes hätten. Über 70 Prozent würden sogar auf die Produkte oder das Unternehmen gänzlich verzichten, wenn dieses sensible Daten weitergibt.[221] Denn eine Datenschutz-Strategie, sichert nicht nur den nachhaltigen Umgang mit Daten, sondern kann Unternehmen dabei verhelfen, einen Wettbewerbsvorteil gegenüber seinen Wettbewerbern zu generieren. Eine solche Strategie signalisiert den Kunden, dass nicht nur auf qualitative Produkte und damit auf die eigene Rentabilität wert gelegt wird, sondern dass auch das Recht des Kunden auf informationelle Selbstbestimmung Berücksichtigung findet („Datenvertrauen"). Dies wiederum schlägt sich in einem niedrigeren Key Issue Score und einem höheren Risk Management Score hinsichtlich des Datenschutzes nieder. Für die Entwicklung einer Datenschutz-Strategie können analog vereinzelte Schritte zur Definition der übergeordneten Unternehmensstrategie mit entsprechenden Abweichungen herangezogen werden. Zur Entwicklung einer Datenschutz-Strategie eignet sich das Fünf-Phasen-Modell, das sich auf die Initiative der Datenschutz-Strategie, Analyse des Unternehmens sowie Umfeldes, Entwicklung, Umsetzung und Überprüfung der Datenschutz-Strategie erstreckt:[222] Hierzu scheint es für viele Unternehmen als unerlässlich, die Unterstützung von Beratern heranzuziehen, um den nachfolgenden Prozess gewissenhaft zu durchlaufen. Im Folgenden werden einzelne Handlungsvorgaben zur Entwicklung und Umsetzung einer Datenschutz-Strategie aufgezeigt, die die Unternehmensberatung bei ihrer Tätigkeit unterstützen. Aus Gründen der Lesbarkeit wurden im Folgenden anstatt „Mandant", die Bezeichnungen „Verantwortlicher", „Unternehmen" u.Ä. verwendet. Jedoch ist damit stets der zu beratende Mandant und dessen Unternehmen gemeint.

Abbildung 14: Prozess für die Entwicklung einer Datenschutz-Strategie.

Eigene Darstellung.

[221] Vgl. *McKinsey (Hrsg.)*, The consumer-data opportunity and the privacy imperative.
[222] In Anlehnung an: *Haake/Rusch/Seiler/Seliner*, Strategie-Workshop, S. 24 ff.

Die Ursachen für die Initiierung einer Strategie im Allgemeinen können vielfältig sein. Allerdings wurde der Auslöser einer Datenschutz-Strategie – und zwar das gesellschaftliche Bedürfnis und die gesetzlichen Anforderungen – behandelt, wodurch diese Phase des Strategiefindungsprozesses nicht ferner behandelt wird.

3.1 2. Schritt: Analyse der strategischen Ausgangslage

Nachdem die Initiative für eine Datenschutz-Strategie im ersten Schritt ergriffen wurde, beginnt der zweite Prozessschritt und damit die Analyse der strategischen Ausgangslage des Unternehmens. Bevor mit der Analyse begonnen werden kann, muss erstmal das übergeordnete Ziel verdeutlicht werden. Hierzu ist eine sog. Vision zu definieren. Eine Vision verkörpert ein Bild der Zukunft, das beschreibt was das Unternehmen in Zukunft erreichen möchte.[223] Eine Vision kann auch im Datenschutzkontext hilfreich sein und kann zur Orientierung während des gesamten Strategieprozesses beitragen. Darüber hinaus hat die Vision auch eine sinnstiftende Funktion, die alle Mitarbeiter zur Umsetzung animieren kann. Eine solche Datenschutzvision hat bereits die Dr. Ing. h. c. F. Porsche AG folgendermaßen definiert: „Privacy – Accelerating Dreams & Innovation!“.[224] Nachdem die Initiative für die Datenschutz-Strategie eingetreten ist und eine Datenschutzvision feststeht, ist das Umfeld sowie das Unternehmen als solches zu analysieren. Im Rahmen dessen sollen sowohl die Anforderungen der relevanten Stakeholder als auch die Stärken und Schwächen des Unternehmens in diesem Kontext ermittelt werden.[225]

3.1.1 Umfeldanalyse

Die Umfeldanalyse beschäftigt sich mit den Geschehnissen in der Wirtschaftslage, Technologie, Ökologie und Gesellschaft eines Unternehmens; hier wird versucht, der Komplexität, Dynamik und der Vernetzung eines Unternehmensumfeldes Genüge zu tun.[226] Ziel ist es, einen Überblick über die aktuelle Situation rund um das Thema Datenschutz zu gewinnen und die Anforderungen der Stakeholder zu eruieren.[227] Der Datenschutz fließt ursprünglich aus dem gesellschaftlichen Bedürfnis heraus und gewinnt stetig mit der zunehmenden Digitalisierung und Konnektivität an Bedeutung. So rückt der ethische Umgang mit Daten ebenfalls in den Fokus globaler Trends, das es zu beachten gilt. Hier könnte eine Fragmentierung der akuten Datenschutzthematiken, die an medialer Präsenz genießen, vorgenommen werden. Bspw. können im Kontext Datenschutz der Datentransfer in Drittstaaten, wie etwa in die USA, akute Themen sein oder auch die Vorratsdatenspeicherung, die sowohl den Triebfedern der entsprechenden Institutionen als auch der Gesellschaft unterliegen.[228] Hierzu können ergänzend zu den Anforderungen aus der DSGVO auch Stellungnahmen der betreffenden Institutionen untersucht werden, um die Anforderungen der Stakeholder in Erfahrung zu bringen. Damit das Unternehmen überdies ein tieferes Verständnis über die Datenschutzawareness der eigenen Zielgruppe und anderer Stakeholder erlangt, bietet sich eine Light-version der Zielgruppen- und Stakeholder-Analyse an. Fragen, die sich das Unternehmen hierzu unter anderem stellen sollte, sind (siehe vollständiger Fragebogen in Anlage 1):

---

[223] Vgl. *Haake/Rusch/Seiler/Seliner*, Strategie-Workshop, S. 40.
[224] *Dr. Ing. h. c. f. Porsche AG (Hrsg.)*, Verantwortung – Geschäfts- und Nachhaltigkeitsbericht der Porsche AG 2021, S. 129.
[225] Vgl. *Haake/Rusch/Seiler/Seliner*, Strategie-Workshop, S. 43.
[226] In Anlehnung an: *Haake/Rusch/Seiler/Seliner*, Strategie-Workshop, S. 43.
[227] Vgl. *Ditlev-Simonsen*, A Guide to Sustainable Corporate Responsibility, S. 155.
[228] Siehe zahlreiche Pressemedien: *Ecovis (Hrsg.)*, Datenübermittlung in die USA? – Jetzt wird bundesweit geprüft; *Handelsblatt (Hrsg.)*, Stefan Brink: „Unternehmen sind mit einer massiven Bußgeldgefahr konfrontiert“; *Datenschutz.org (Hrsg.)*, Vorratsdatenspeicherung – Stehen alle Menschen unter Generalverdacht?.

1. Über welchen Bildungsstand verfügt die Zielgruppe? Z.B. kann ein höherer Bildungsstand eine erhöhte Sensibilität für den Datenschutz bedingen, das kann wiederum zu erhöhten Ansprüchen führen.
2. Welches Alter hat die Zielgruppe? Während Generation X und Y wahrscheinlich ein niedrigeres Bewusstsein haben und demnach eine höhere Aufklärung voraussetzen, wird bei Generation Z eine höhere Awareness angenommen.
3. Wie viele Betroffenenanfragen erhält das Unternehmen im Durchschnitt? Die Anzahl der Betroffenenanfragen kann ein Indikator für die Relevanz des Datenschutzes der eigenen Zielgruppe sein. Auch Meldungen von Datenschutzverstößen an die Aufsichtsbehörde durch die Betroffenen können herangezogen werden.
4. Welche Norm betreffen die Betroffenenanfragen? Welches Betroffenenrecht am meisten durch die Betroffenen ausgeübt wird, ermöglicht herauszufinden, worauf die Betroffenen hinsichtlich des Datenschutzes besonderen Wert legen.

3.1.2 Unternehmensanalyse

Nachdem das Umfeld des Unternehmens analysiert wurde, sind die Stärken und Schwächen des Unternehmens zu untersuchen und mit den datenschutzrechtlichen Anforderungen abzugleichen.[229] Dadurch wird eine Ausrichtung der Datenschutz-Strategie entsprechend der vorangegangenen Umfeldanalyse möglich. Hierbei liegt das Augenmerk insbesondere auf der Geschäftstätigkeit des Unternehmens sowie auf der Sensibilität der Verarbeitungsvorgänge und Kenntnis des eigenen Datenschutzstandards.[230] Die Unternehmensanalyse unterliegt dabei dem in Abbildung 15 definierten Prozess und beginnt mit der Analyse des Unternehmensprofils gefolgt von der Gap- und SWOT-Analyse.[231]

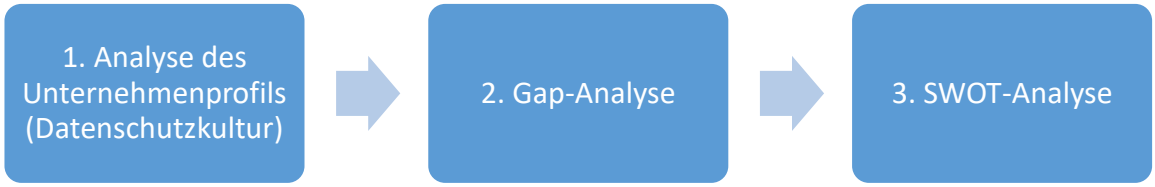

Abbildung 15: Vorgehensweise der Umfeldanalyse.

Eigene Darstellung.

Die Analyse des Unternehmensprofils gibt Aufschluss darüber, wie das Unternehmen und dessen Mitarbeiter den ethischen Umgang mit Daten als Wert einbeziehen und wie dieses umgesetzt wird. Vor diesem Hintergrund sind Unternehmenswerte ein unabdingbares Mittel zur Analyse des Unternehmens. Als Instrument kann das Erstellen eines Kulturprofils des Unternehmens dienen. Zuerst werden die maßgeblichen Kriterien festgelegt, um den Ist-Zustand erheben zu können. Maßgebliche Kriterien können bspw. sein, dass der Grundsatz der Datenminimierung konsequent gewahrt wird, sodass keine nicht notwendigen Daten verarbeitet werden. Oder aber auch, dass kein Datentransfer in unsichere Dritt-

[229] Vgl. *Haake/Rusch/Seiler/Seliner*, Strategie-Workshop, S. 55 ff.
[230] Vgl. *Voigt/von dem Bussche*, EU-Datenschutzgrundverordnung (DSGVO) – Praktikerhandbuch, S. 322.
[231] In Anlehnung an: *Haake/Rusch/Seiler/Seliner*, Strategie-Workshop, S. 55 ff.; *Voigt/von dem Bussche*, EU-Datenschutzgrundverordnung (DSGVO) – Praktikerhandbuch, S. 322.

länder stattfindet. Stets von Bedeutung ist es dabei, die Kriterien im Lichte der Umfeldanalyse festzulegen, sodass den Ansprüchen der Stakeholder begegnet werden kann. Anschließend wird analysiert, wie weit die einzelnen Aussagen im Unternehmen aktuell gelebt werden. Zur Erlangung dieser Informationen können Fragebogen eingesetzt werden, in dem die Mitarbeiter ihre Einschätzung von trifft zu bis gar nicht angeben können. Dabei gilt zu beachten, dass die theoretischen Werte von den tatsächlich gelebten Werten devieren. Die Diskrepanz zwischen dem Ist- und dem Soll-Zustand zeigt, welche Aspekte in die Strategiefindung besonders berücksichtigt werden müssen.[232] Wird bspw. angegeben, dass so viele Daten wie möglich erhoben werden, um die Produkte besser zu vermarkten, kann das Unternehmen daraus schlussfolgern, dass Schulungs- und Sensibilierungsmaßnahmen einen erheblichen Bestandteil der Strategie darstellen sollte.

3.1.2.1 GAP-Analyse

Zur Ermittlung des tatsächlichen Datenschutzstandards wird die sog. Gap-Analyse, auch als Lücken-Analyse bekannt, eingesetzt. Ziel der Gap-Analyse ist es, bestehende Defizite im Datenschutz zu identifizieren und in selbem Zuge zu beseitigen.[233] Die bereits bestehende Task-Force sieht sich in diesem Prozess in enger Zusammenarbeit mit den verantwortlichen Personen der einzelnen Fachbereiche des Unternehmens. Der Kernunterschied zur Analyse des Unternehmensprofils ist, dass die GAP-Analyse über eine höhere Granularität verfügt und der tatsächliche Umgang mit den Daten im Unternehmen ermittelt wird. Methoden zur Durchführung der Gap-Analyse können Workshops, spezielle Befragungen oder Selbsteinschätzungen sein. Im Rahmen dessen werden im ersten Schritt alle Verarbeitungsvorgänge und die Verarbeitungszwecke ermittelt. Daraufhin sind die bestehenden Datenschutzmaßnahmen zu untersuchen. Folglich sollte die Gap-Analyse unter den folgenden Gesichtspunkten erfolgen: [234]

- Welche *Verarbeitungsvorgänge* zu welchen *Zwecken* durchgeführt werden;
- welche *Arten von Daten* verarbeitet werden;
- wie die *Verantwortlichkeiten intern verteilt* sind;
- welche *Datenschutzmaßnahmen* vorhanden sind, unter anderem was die Rechte
- der betroffenen Personen betrifft; und
- welche Quellen vergangene Datenschutzverstöße verursacht haben.

Parallel sind in der Gap-Analyse auch die Pflichten des Unternehmens nach der DSGVO auf Grundlage der jeweiligen Verarbeitungstätigkeiten zu identifizieren. Anschließend vergleicht das Unternehmen die bestehenden Datenschutzstandards mit den neuen Datenschutzpflichten und erkennt so die bestehenden Schutz-„Lücken“, die im Rahmen des Datenschutzrisikomanagements (siehe unten) geschlossen werden.[235] Überdies können auch die Bausteine des Standarddatenschutzmodells einen erheblichen Beitrag zur Ermittlung von Defiziten leisten. Die Datenschutz-GAP-Analyse kann dabei in folgende Bereiche untergliedert werden, wonach auch die Prüfung anhand von Fragebögen stattfinden kann, die in Anlage 2 zu finden ist[236]:

---

[232] Vgl. *Haake/Rusch/Seiler/Seliner*, Strategie-Workshop, S. 69.
[233] Vgl. *Voigt/von dem Bussche*, EU-Datenschutzgrundverordnung (DSGVO) – Praktikerhandbuch, S. 322.
[234] Vgl. *Voigt/von dem Bussche*, EU-Datenschutzgrundverordnung (DSGVO) – Praktikerhandbuch, S. 322.
[235] Vgl. *Voigt/von dem Bussche*, EU-Datenschutzgrundverordnung (DSGVO) – Praktikerhandbuch, S. 322.
[236] In Anlehnung an Kapitel 2-5 der DSGVO; *Kretzmann*, Analyse und Implementierung eines Datenschutzmanagementsystems (DSMS) gemäß Datenschutz-Grundverordnung (DSGVO) in ein

1. Grundsätze des Datenschutzes: Hierbei werden die in der DSGVO vorgesehenen Datenschutzgrundsätze geprüft. Diese sind die Rechtmäßigkeit der Verarbeitung, Datenminimierung, Zweckgebundenheit, Transparenz, Richtigkeit der Daten, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Treu und Glauben.

2. Rechte der betroffenen Personen: In diesem Kontext ist der Prozess zur Beantwortung von Betroffenenanfragen zu prüfen und die Beantwortung als solches. Hiervon umfasst sind das Auskunftsrecht, Recht auf Löschung, Recht auf Berichtigung, Recht auf Einschränkung, Recht auf Widerspruch und Recht auf Datenübertragbarkeit, Art. 14 ff. DSGVO.

3. Datenschutzrechtliche Verträge: Prüfungsgegenstand sind hier die Verträge mit den Auftragsverarbeitern und gemeinsamen Verantwortlichen. Das Hauptaugenmerkmal liegt insbesondere auf die datenschutzrechtliche Vertragsgestaltung und auf der Vereinbarung der TOMs.

4. Datenübermittlung an Drittländer oder an internationale Organisationen: Abgefragt werden die Übermittlungen der Daten in sichere oder unsichere Drittländer, darunter auch, welche Länder, welche Daten usw. davon betroffen sind.

Die Ergebnisse der GAP-Analyse lassen sich mittels Excel visuell darstellen und identifiziert die herrschenden Defizite.

3.1.2.2 SWOT-Analyse

Nachdem die Defizite mittels der GAP-Analyse identifiziert wurden, ist ein Stärken-/Schwächenprofil anhand einer SWOT-Analyse zu erstellen. In der Betriebswirtschaft wird die SWOT-Analyse als eine interne Analyse der Stärken (Strengths) und Schwächen (Weaknesses) sowie über eine externe Analyse der Möglichkeiten (Opportunities) und Risiken (Threats) verstanden. Daneben gewinnen Unternehmen einen Überblick darüber, wie sie sich am Markt positionieren können und welche Schwächen behoben werden müssen. Eine SWOT-Analyse dient nicht nur der strategischen Positionierung eines gesamten Unternehmens, sondern kann auch auf einzelne Geschäftsbereiche – wie etwa dem Datenschutz – angewendet werden.[237] Allerdings ist die SWOT-Analyse mit Hinblick auf den Datenschutz einigen Grenzen ausgesetzt. Auch wenn bspw. die Zielgruppe eines Unternehmens keinen besonderen Anspruch an den Schutz personenbezogener Daten hat, sind die regulatorischen Anforderungen dennoch zu erfüllen. Die SWOT-Analyse hilft also Unternehmen den Datenschutz entsprechend endogener Faktoren wie den Stärken und Schwächen sowie exogener Faktoren wie Gefahren und Chancen strategisch und damit auch nachhaltig zu gestalten. Hieraus lassen sich sodann strategische Ausrichtungen ableiten.[238] Für die Optimierung der technischen und organisatorischen Maßnahmen ist es förderlich, diese auch der SWOT-Analyse zu unterziehen, zumal sie ein vielaussagender Indikator für den bestehenden Datenschutzstandard sind. Die folgende Abbildung zeigt beispielhaft eine SWOT-Analyse bzgl. des Datenschutzes für einen Automobilhersteller auf. Zur Ermittlung der einzelnen Kriterien können die Ergebnisse aus der GAP-Analyse komplementär herangezogen werden, jedoch ist auch hier der enge Austausch mit den Fachbereichen notwendig. Stärken geben sich aus internen Faktoren des Unternehmens heraus. Hierunter kann z.B. eine gute Beziehung mit der zuständigen Datenschutzaufsichtsbehörde fallen oder aber auch umfassende datenschutzrechtliche Verträ-

bestehendes Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 am Beispiel eines mittelständischen Unternehmens, S. 30.

[237] Vgl. *Schawel/Billing*, Top 100 Management Tools, S. 249.

[238] Vgl. *Haake/Rusch/Seiler/Seliner*, Strategie-Workshop, S. 53.

ge mit den Dienstleistern und gemeinsamen Verantwortlichen. Ferner ist ein effektiver Betroffenenrechteprozess förderlich für die Außenkommunikation mit den Betroffenen und stärkt das Vertrauen in eine ethische und nachhaltige Verarbeitungspraktik. Als Schwächen können bspw. die eigenen Produkte identifiziert werden, wenn diese massenhaft (besondere) personenbezogene Daten verarbeiten und der Kunde bspw. nicht autonom bestimmen kann, welche Daten verarbeitet werden sollen. Dies ist insbesondere dann der Fall, wenn bspw. (teil-)autonome Fahrzeuge eingesetzt oder Connected-Car-Services angeboten werden, die eine kontinuierliche Erfassung des Fahrzeugstandortes voraussetzen. Wie bereits oben thematisiert wurde, ist eine solche massenhafte Verarbeitung nicht alleinig auf das berechtigte Interesse des Automobilherstellers zu stützen. Um die Nutzung und die Effektivität der Dienste zu gewährleisten sowie die zur Verfügungstellung der Daten durch den Kunden zu forcieren, sind weitere datenschutzrechtliche Maßnahmen erforderlich. Aber auch Dienstleister in Drittländern und damit die Datenübermittlung in unsichere Drittländer, Schulungsdefizite sowie Verstöße gegen die DSGVO stellen Schwächen eines Unternehmens dar.

Chancen und Gefahren hingegen ergeben sich aus dem externen Umfeld eines Unternehmens. Ein Unternehmen kann bspw. die Chance nutzen und durch Etablierung eines Consent-Managers im Infotainmentsystem die Datensouveränität des Kunden erhöhen. Dies wiederum verstärkte das Datenvertrauen des Kunden. Auf diese Weise entsteht eine Win-Win-Situation, denn durch das verstärkte Datenvertrauen kann auch die Bereitschaft des Betroffenen steigen, seine personenbezogenen Daten zur Nutzung der Dienste bereitzustellen. Folglich gewährt dies dem Verantwortlichen ein Alleinstellungsmerkmal auf dem Markt, wodurch gewisse Wettbewerbsvorteile generiert werden. Threats stellen Gefahren für das Unternehmen und dessen Erfolg dar. Der Verlust des Datenvertrauens stellt dahingehend eine Gefahr dar, da hierdurch die Kunden entweder die Datenbereitstellung reduzieren oder gar die Produkte gänzlich vermeiden. In einer Kettenreaktion kann ein Datenschutzverstoß die Zahlung von Bußgeldern, Klagen von Betroffenen, Reputationsschäden oder eine Veränderung der Gesetzeslage nach sich ziehen.

Datenschutz-SWOT-Analyse	
Intern	**Extern**
S = Strengths („Stärken“) • Rege Kommunikation mit der Datenschutzaufsichtsbehörde • Umfassende Auftragsverarbeitungsverträge mit Auftragsverarbeitern oder gemeinsamen Verantwortlichen • Effizienter/Effektiver Betroffenenrechteprozess • Datenschutzmanagementsystem	**O = Opportunities („Chancen“)** • Erhöhung des Datenvertrauens der Kunden durch „Datensouvernität“ • Mehrwert für den Kunden und dadurch Bereitschaft höher, personenbezogene Daten zur Verarbeitung zur Verfügung zu stellen • Alleinstellungsmerkmal auf dem Markt und dadurch Sicherung eines Wettbewerbsvorteils
W = Weaknesses („Schwächen“) • Massenhafte Verarbeitung personenbezogener Daten durch autonome Fahrzeuge und Connected-Car-Services • Datenübermittlung in unsichere Drittländer • Schulungsdefizite im Datenschutz • Fehlende Datenschutzorganisation	**T = Threats („Gefahren“)** • Verlust des „Datenvertrauens“ der Kunden • Zahlung von Bußgeldern und Klage • Reputationsschaden durch Veröffentlichung • Veränderung der Gesetzeslage zu Ungunsten der Verantwortlichen

Abbildung 16: SWOT-Analyse.

Eigene Darstellung in Anlehnung an: Cobra CRM (Hrsg.), CRM und Datenschutz – ziemlich beste Freunde!.

3.2 3. Schritt: Formulierung der Datenschutz-Strategie

Anhand der Analyseergebnissen aus Schritt zwei werden nun strategische Alternativen und Handlungsoptionen ausgelotet, die erfolgversprechendste Variante ausgewählt und die Strategie daraufhin ausformuliert. Die Strategieformulierung genannt auch Strategieentwicklung gibt die zukünftige Entwicklungsrichtung des Unternehmens an. Als Grundlage dient die Unternehmens- und Umfeldanalyse. Grundsätzlich gibt es zwei Ebenen, auf

der Strategien gebildet werden: zum einen auf der Ebene der Geschäftseinheit und auf der Ebene des Unternehmens. Während Strategien der Geschäftseinheiten die Art und Weise bestimmen, wie das Unternehmen in den einzelnen Geschäftsfeldern im Wettbewerb bestehen soll, legt eine Unternehmensstrategie das Betätigungsfeld des Unternehmens im Gesamten fest.[239] Ziel der Unternehmensstrategie ist vielmehr die Führung der Geschäftsfelder.[240] Fraglich in diesem Kontext ist jedoch, welche der beiden Ebenen sich zur Entwicklung einer Datenschutz-Strategie eignet. Zwar bildet die Datenschutzabteilung eine separate Einheit in der gesamten Organisation, jedoch handelt es sich hierbei nicht um ein Geschäftsfeld, welches operativ zur Unternehmensleistung beiträgt. Da sich die Verarbeitung von personenbezogenen Daten über viele Einheiten eines Unternehmens hinwegzieht (bspw. Personalabteilung, Beschaffung/Einkauf und Vertrieb) handelt es sich beim Datenschutz um ein Anliegen, welches – als Teil der ESG-Strategie – einen Bestandteil der Unternehmensstrategie darstellen sollte. Die Datenschutz-Strategie sollte daher einen klaren Pfad für jede einzelne Geschäftseinheit bieten sowie die Führung und Kontrolle jeder einzelnen Geschäftseinheit ermöglichen.[241] Die Entwicklung einer generischen Datenschutz-Strategie postuliert die Priorisierung von Handlungsfeldern, die Festlegung der strategischen Stoßrichtungen und die Definition entsprechender Ziele.

3.2.1.1 Priorisierung der Handlungsfelder

Die vorgehenden Analysen werden in der Regel eine Reihe an Ergebnissen mit bestimmten Handlungsfeldern liefern. Damit jedoch der Datenschutz-Strategie eine Struktur innewohnt, sind die ermittelten Handlungsfelder rudimentär zu priorisieren. Zudem scheint es empfehlenswert die Handlungsfelder anhand den beiden Kenngrößen Aufwand und Nutzenpotenziale zu evaluieren, um später auch die Budgetplanung zu unterstützen. Zur Bewertung bieten sich diverse Hilfsmittel an, die je nach Unternehmen individuell ausgewählt werden können. Die Priorisierung wird auch von der Kritikalität der Schwäche oder der Gefahr tangiert, wodurch es von hoher Bedeutung ist, dieses Kriterium in die Bewertung zu involvieren.[242] Die Priorisierung der Handlungsfelder im Datenschutz kann bspw. analog zu der Kategorisierung aus dem Informationsmanagement erfolgen (siehe Abbildung 17).

[239] Vgl. *Lombriser/Abplanapl*, Strategisches Management, S. 267.
[240] Vgl. *Wicharz*, Strategie: Ausrichtung von Unternehmen auf die Erfolgslogik ihrer Industrie, S. 215.
[241] Vgl. *Matzler/Müller/Mooradian-Seeger/Hautz/Mooradian*, Strategisches Management, S. 25.
[242] Vgl. *Schuh/Zeller/Stich*, Digitalisierungs- und Informationsmanagement, S. 113.

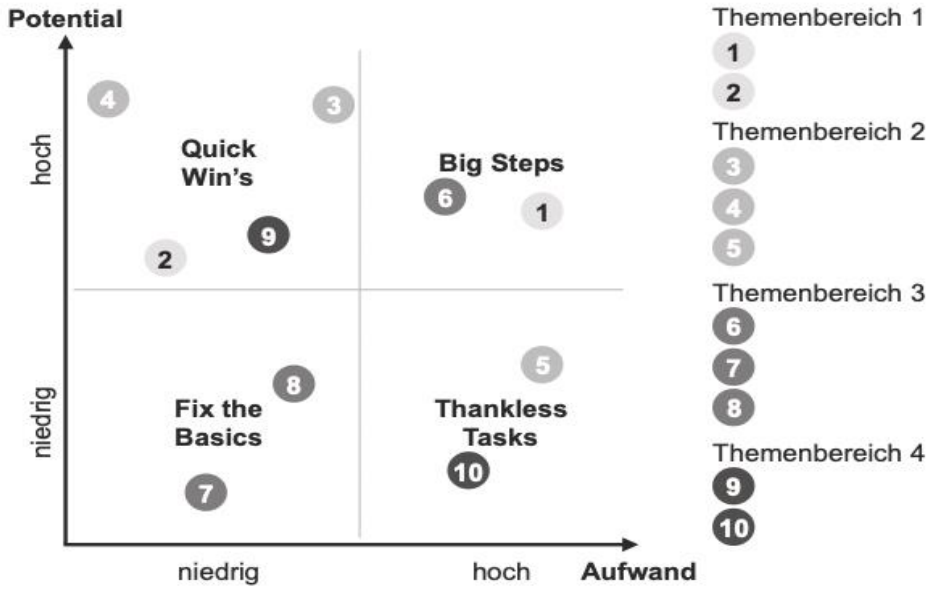

Abbildung 17: Schematische Darstellung priorisierter Handlungsfelder.

Schuh/Zeller/Stich, Digitalisierungs- und Informationsmanagement, S. 113.

3.2.1.2 Strategische Stoßrichtungen

Basierend auf der SWOT-Analyse lassen sich für die Kombinationen Chancen/Gefahren und Stärken/Schwächen vier strategische Stoßrichtungen ableiten, die in der TOWS-Matrix (Threats, Opportunities, Weaknesses, Strenghts)[243] behandelt werden. Bei der Erstellung der TOWS-Matrix werden 5-10 höchstpriorisierte Stärken, Schwächen, Chancen und Gefahren von der SWOT-Analyse übertragen. Daraufhin sind die Korrelationen zwischen den einzelnen Faktoren aus der SWOT-Analyse zu eruieren (positive/negative/keine Korrelation). Mit diesen Erkenntnissen werden sodann die geeigneten strategischen Stoßrichtungen abgeleitet (SO, WO, ST, WT). Abschließend ist eine Gesamtauswirkung der einzelnen Maßnahmen und Faktoren vorzunehmen, die den Gesamtnutzen bzw. -risiko und dadurch der Mehrwert je Stoßrichtung ermittelt wird.[244] Folgende Handlungsoptionen stehen dabei zur Wahl: [245]

1. **Matching-Strategie (SO-Strategie):** Nutzung der Stärken, um Chancen zu realisieren
2. **Umwandlungsstrategie (ST-Strategie):** Stärken nutzen, um Gefahren abzuwehren
3. **Neutralisierungsstrategie (WO-Strategie):** Schwächen beheben, um Chancen zu nutzen
4. **Verteidigungsstrategie (WT-Strategie):** Schwächen beheben, um Gefahren abzuwehren

[243] Vgl. *Ehringer*, Instrumente zur Strategieentwicklung: methodische Unterstützung für Praktiker, S. 41.
[244] Vgl. *Ehringer*, Instrumente zur Strategieentwicklung: methodische Unterstützung für Praktiker, S. 42.
[245] Vgl. *Haake/Rusch/Seiler/Seliner*, Strategie-Workshop, S. 54; *Ehringer*, Instrumente zur Strategieentwicklung: methodische Unterstützung für Praktiker, S. 41.

		Interne Faktoren	
		Stärken	**Schwächen**
Externe Faktoren	**Chancen**	***SO-Strategie***	***WO-Strategie***
	Risiken	***ST-Strategie***	***WT-Strategie***

Abbildung 18: TWOS-Matrix.

In Anlehnung an: Weihrich, The TWOS-Matrix – A Tool for Situational Analysis, S. 60; Ehringer, Instrumente zur Strategieentwicklung: methodische Unterstützung für Praktiker, S. 42.

Eine **Matching-Strategie** kommt dann in Betracht, wenn die Stärke einer guten Beziehung zu den zuständigen Datenschutzaufsichtsbehörden eine enge Zusammenarbeit hinsichtlich neuer Produkte und der datenschutzkonformen Ausgestaltung ermöglicht. Hierdurch ließe sich dann die Zusammenarbeit weiter intensivieren, was die Akzeptanz und die Toleranz der Aufsichtsbehörden von neuen Produkten und Verarbeitungsvorgängen positiv beeinflusst. Weiterhin können ein effizienter Betroffenenrechteprozess sowie ein Datenschutzmanagementsystem gegen Datenschutzverstöße und damit Reputationsschäden präventiv wirken, da diese in der Regel eine frühzeitige Identifizierung von Defiziten ermöglichen – in diesem Fall handelt es sich um eine **Umwandlungsstrategie**. Bei der **Neutralisierungsstrategie**[246] können beispielsweise Dienstleister in unsicheren Drittländern vermieden und dafür europäische Alternativen herangezogen werden, um das Datenvertrauen der Kunden zu gewinnen. Auf diese Weise wird somit die Schwäche Datenübertragung in unsichere Drittländer neutralisiert und es kann der Chance, ein Alleinstellungsmerkmal auf dem Mark zu gewinnen, nachgegangen werden. Eine Strategie zur Verteidigung sog. **Verteidigungsstrategie**[247] wird dann in Erwägung gezogen, wenn Schwächen behoben werden, um Bedrohungen abzuwehren. Dies ist z.B. dann der Fall, wenn die Schulungsdefizite der Mitarbeiter durch weitere Schulungsmaßnahmen eliminiert werden, um einen Datenschutzverstoß vorzubeugen. Bemerkenswert bei der Definition von einer strategischen Stoßrichtung ist, dass eine Stoßrichtung zwei oder gar mehrere Strategien beinhalten kann und somit Korrelationen aufweist. Werden bspw. Schulungsdefizite behoben, um Datenschutzverstöße zu vermeiden, kann gleichzeitig eine Chance ausgenutzt werden und damit den Mehrwert für den Kunden erhöhen. Viele Schwächen setzen unmittelbare Maßnahmen des Unternehmens voraus. Damit jedoch der Datenschutz-Strategie-Prozesses nicht gestört wird, sind solche Sofortmaßnahmen zu notieren und zu priorisieren. Diese sollten dann im Rahmen des operativen Geschäfts oder des Maßnahmenplanes der Strategieumsetzung umgesetzt werden.[248]

[246] Vgl. *Haake/Rusch/Seiler/Seliner*, Strategie-Workshop, S. 54; *Ehringer*, Instrumente zur Strategieentwicklung: methodische Unterstützung für Praktiker, S. 42.
[247] Vgl. *Haake/Rusch/Seiler/Seliner*, Strategie-Workshop, S. 54.
[248] Vgl. *Haake/Rusch/Seiler/Seliner*, Strategie-Workshop, S. 55.

3.2.1.3 Zielformulierung

Da strategische Stoßrichtungen und Strategien in der Regel nur durch konkrete Ziele umsetzbar sind, sind solche aus den Handlungsfeldern abzuleiten. Hierzu werden die Ziele entsprechend der Rangfolge (hohe Priorität bis niedrige Priorität) peu a peu abgearbeitet. Datenschutz-Ziele können dabei sowohl technische und organisatorische als auch prozessuale und kulturelle Aspekte inkludieren. Mittels des OGTM-Frameworks (Objectives, Goals, Tactics and Measures) lassen sich konkrete Ziele definieren. Dabei sind Objectives allgemeine Zielsetzungen. Solche allgemeinen Zielsetzungen werden kompakt beschrieben und stellen das übergeordnete Ziel dar. Als übergeordnetes Ziel gilt es, einen Überblick über alle Dienstleister zu gewinnen, um diese zum einen zu verwalten und zum anderen die Quote der Dienstleister mit Sitz im unsicheren Drittland zu reduzieren. Diese Ziele werden dann ferner konkretisiert, wodurch sie als „Goals" bezeichnet werden. Diese sind gemäß dem SMART-Prinzip – also spezifisch, messbar, akzeptiert, realistisch und terminiert – zu definieren.[249] Beispielsweise kann die Implementierung eines Contractmanagementsystems in das bestehende Datenschutzmanagementsystem zur Verwaltung aller Dienstleister als Goal gelten. Ferner könnte eine konkrete Zielsetzung sein, die Dienstleister, die im unsicheren Drittland sitzen durch europäische Dienstleister zu ersetzen. Oder aber auch die Überprüfung der datenschutzrechtlichen Verträge und TOMs. Goals und Objectives erfordern zudem dezidierte Aktionen (Tactics), die zur Erreichung der Ziele beitragen sollen. Tactics sind dabei als Ideenspeicher anzusehen, in dem initiale Aktionen zur Zielerreichung, insbesondere in Bezug auf die zuvor hergeleiteten Herausforderungen, beitragen sollen. Da es sich hierbei um eine initiale Erfassung von Tactics handelt, erfordert es keiner Kategorisierung oder Rangfolge. Für die Bereinigung der Dienstleister mit Sitz in unsicheren Drittländern sind bspw. im ersten Schritt jene Dienstleister zu identifizieren und simultan eine Recherche zu der Möglichkeit eines Contractmanagementsfeatures und den Konditionen zu betreiben.

Zuletzt sind Measures messbare Metriken für die Tactics zu erfassen. Es werden den bis dato noch nicht messbaren Zielen quantitative Kriterien wie etwa Mengen, Prozentzahlen oder auch Fristen beigefügt, sodass der Stand der Zielerreichung jederzeit nachvollzogen werden kann.[250] So kann man bspw. festlegen, dass die Implementierung des Contractmanagementsystems bis zum 2. Quartal 2023 stattzufinden hat, sodass auf Basis dessen ein Projektplan erstellt wird. Es kann aber auch eine Reduktion von 10% der Dienstleister mit Sitz im unsicheren Drittland festgesetzt werden. Die Frequenz der jährlichen Überprüfung der datenschutzrechtlichen Verträge und einiger TOMs richtet sich nach den gesetzlichen Vorschriften. Allerdings ist hier zu betonen, dass die jährliche Überprüfung nicht bei allen TOMs ausreichend ist. Die Feststellung der Wirksamkeit einer Firewall bedarf einer häufigeren Prüfung in kürzeren Zeitabständen.[251] Tactics und Measures dienen daneben als Vorbereitung auf die folgende Umsetzungsphase der Strategie.[252]

[249] Vgl. *Schuh/Zeller/Stich*, Digitalisierungs- und Informationsmanagement, S. 114.
[250] Vgl. *Schuh/Zeller/Stich*, Digitalisierungs- und Informationsmanagement, S. 115.
[251] Vgl. *Datenschutzbeauftragter Hamburg (Hrsg.)*, Das Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der TOM.
[252] Vgl. *Schuh/Zeller/Stich*, Digitalisierungs- und Informationsmanagement, S. 115.

Objectives (Zielsetzung)	**Goals (Ziele)**
Verwaltung und Übersicht der Dienstleister und datenschutzrechtliche Verträge Reduzierung der Dienstleister mit Sitz im unsicheren Drittland	Implementierung eines Contractmanagementfeatures in das bestehende Datenschutzmanagementsystem Regelmäßige Aktualisierung der Verträge bzw. TOMs Ausweichung auf europäische Alternativen
Tactics (mögliche Aktionen)	**Measures (messbare Metriken)**
Recherche nach Contactsmanagementfeatures und Einholung von Angeboten Identifikation der Dienstleister mit Sitz im unsicheren Drittland Recherche von und Verhandlung mit europäischen Dienstleistern	Implementierung des Contractmanagementsystems bis zum 2. Quartal 2023 Reduzierung der Dienstleister mit Sitz im unsicheren Drittland um 10% bis zum Ende des Jahres Jährliche Überprüfung und Aktualisierung der TOMs

Abbildung 19: Framework für die Zieldefinition anhand eines Beispiels.

Schuh/Zeller/Stich, Digitalisierungs- und Informationsmanagement, S. 114.

3.3 4. Schritt: Umsetzung der Datenschutz-Strategie

Ist die Erarbeitung der Strategie abgeschlossen, muss diese in die Praxis umgesetzt werden. Eine erfolgreiche Umsetzung setzt voraus, dass die entwickelte Strategie operationalisiert und auf konkrete Maßnahmen heruntergebrochen wird.[253] Zu bemerken ist jedoch, dass der Umsetzungsprozess einer Strategie im Gegensatz zum Entwicklungsprozess nicht ausschließlich auf rationale Aspekte beruht, sondern auch von irrationalen Faktoren flankiert wird.[254] Demnach kann sich dieser Prozessschritt von Unternehmen zu Unternehmen stark unterscheiden. Insbesondere die Umsetzung der Datenschutz-Strategie erfordert das Commitment aller Mitarbeiter, wodurch Schulungen, Kommunikation etc. an besonderer Bedeutung gewinnen.

3.3.1 Gründung einer Datenschutzorganisation mit Schnittstelle zu ESG

Die Umsetzung der Datenschutz-Strategie erfordert grundsätzlich eine Organisationseinheit, die sich zu einen mit dem grundlegenden Fragen des Datenschutzes beschäftigt und der zum anderen auch die nachhaltige Umsetzung der Strategie obliegt. Abhängig von der Unternehmensgröße, Struktur, Produktportfolie, Geschäftsmodelle etc. sind daher Rollen, Verantwortlichkeiten, Kompetenzen und Gremien[255] zur Umsetzung der Datenschutz-Strategie festzulegen. Unter einer Datenschutzorganisation definiert man die Aufbauorganisation eines Unternehmens oder einer Unternehmensgruppe, welcher die Aufgabe hat, die Anforderungen gemäß der DSGVO durchzusetzen. Eine Datenschutzorganisation zieht sich durch sämtliche Hierarchieebenen eines Unternehmens durch und

[253] Vgl. *Haake/Rusch/Seiler/Seliner*, Strategie-Workshop, S. 117.
[254] Vgl. *Lombriser/Abplanapl*, Strategisches Management, S. 375.
[255] Vgl. *Hanschke*, Informationssicherheit und Datenschutz, S. 86.

reicht von den einzelnen Geschäftsbereichen bis zu der Top-Management-Ebene. Eine Datenschutzorganisation kann zum einen dedizierte Rollen wie Datenschutzbeauftragte(n), Datenschutz-Koordinatoren und Datenschutzexperten umfassen. Allgemein sollte gewährleistet werden, dass die datenschutzrechtlichen Vorgaben rollenspezifisch in allen Tätigkeiten im Unternehmen berücksichtigt werden, die die Verarbeitung personenbezogener Daten zum Gegenstand haben. Darüber hinaus ist es unerlässlich, dass durch die Datenschutzorganisation eine effiziente Zusammenarbeit zwischen den einzelnen Rollen gewährleistet wird. Eine solche Datenschutzorganisation findet sich in Abbildung 20 wieder.

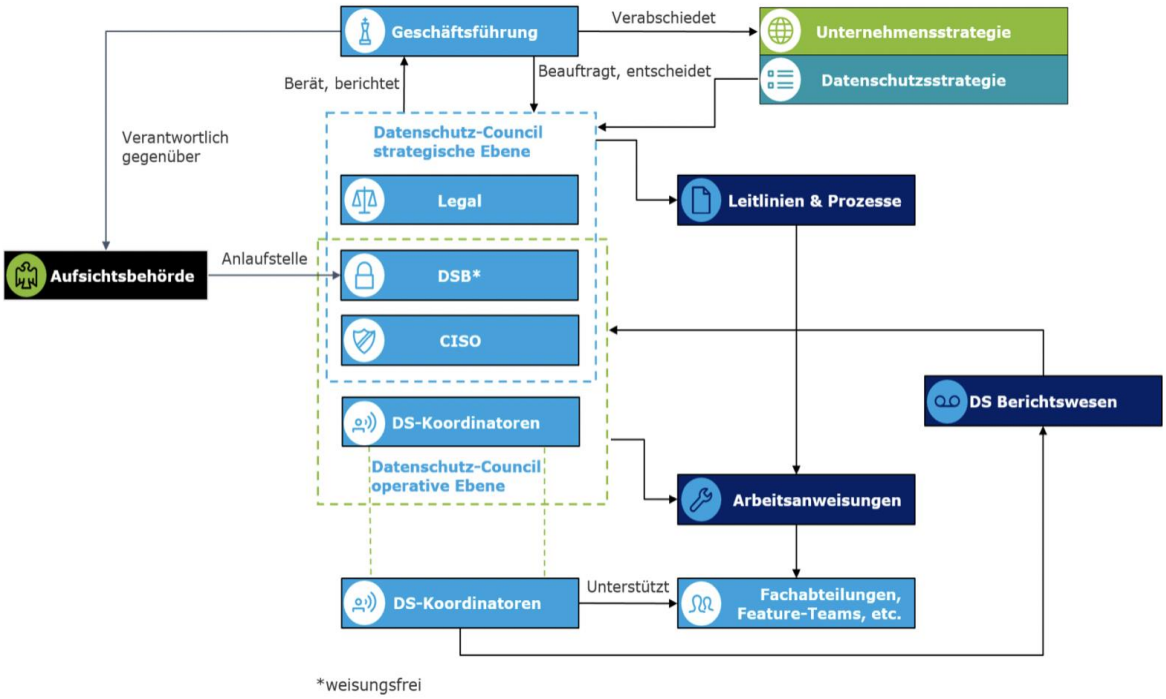

Abbildung 20: Schematischer Aufbau einer Datenschutz-Organisation.

Deloitte (Hrsg.), Datenschutz-Organisation, online abrufbar unter: https://www2.deloitte.com/de/de/pages/risk/articles/datenschutz-organisation.html, zuletzt besucht am 28.09.2022.

Der/die Datenschutzbeauftragte hat in der Datenschutzorganisation eine gesonderte Position. Das liegt daran, dass ihn zum einen die Beratungsfunktion hinsichtlich datenschutzspezifischer Fragen des Unternehmens obliegt und zum anderen fingiert er als Kontaktperson für die Aufsichtsbehörde. Zu unterstreichen ist dabei, dass der/die Datenschutzbeauftragte stets weisungsfrei und unabhängig agieren muss, Art. 38 DSGVO. Im Rahmen der Tätigkeit als Datenschutzbeauftrage(r) berichtet er/sie unmittelbar an die Geschäftsführung und unterrichtet sie über den aktuellen Status des Datenschutzes im Unternehmen. Die Tätigkeit des Datenschutzbeauftragten beinhaltet ferner die Unterrichtung und Beratung der Geschäftsführung und der Mitarbeiter hinsichtlich ihrer Pflichten und die Überwachung und Beratung bei Datenschutzfolgeabschätzungen gem. Art. 35 DSGVO.

Datenschutzkoordinatoren stellen indes den verlängerten Arm des Datenschutzkoordinatoren dar und unterstützen dabei, Datenschutzthematiken in den jeweiligen Fachabteilungen zu treiben und umzusetzen. Die Etablierung von Datenschutzkoordinatoren führt zu einer effizienteren Umsetzung der Vorgaben, aber vor allem auch zu einer unmittelbaren

Beantwortung datenschutzspezifischer Fragestellungen seitens der Mitarbeiter. Die Aufgabe des Datenschutzkoordinatoren besteht darin, die Datenschutz-Compliance in der eigenen Abteilung zu gewährleisten. Häufig verfügen Datenschutzkoordinatoren über das fachspezifische Know-How, weshalb ihnen insbesondere die Verantwortung obliegt, das Verarbeitungsverzeichnis des eigenen Verantwortungsbereichs zu befüllen und zu pflegen. Auch bei der Durchführung von Datenschutz-Folgenabschätzungen oder bei Privacy by Design wirken Datenschutzkoordinatoren mit. Darüber hinaus müssen diese nach Kenntnisnahme eines Datenschutzverstoßes entsprechend agieren und den/die Datenschutzbeauftragten konsultieren, sodass eine Bewertung des Risikos für die Betroffenen durchgeführt werden kann. Ferner nehmen Datenschutzkoordinatoren auch die Stellung als Datenschutzbotschafter, wodurch diese des weiteren das Ziel verfolgen, die Datenschutzkultur innerhalb ihrer Abteilung und im gesamten Unternehmen zu fördern. Anders als bei dem/r Datenschutzbeauftragten oder der Geschäftsführung wirken die Datenschutzkoordinatoren nicht bei der Entwicklung der Datenschutz-Strategie mit, sondern sind vielmehr für operative Ausführung dieser zuständig. Unter anderem können den Datenschutzkoordinatoren noch die Sicherstellung der Einhaltung von Richtlinien und Arbeitsanweisungen oder die Mitwirkung bei Datenschutzaudits zugewiesen werden. Wichtig dabei ist stets, dass die Datenschutzkoordinatoren entsprechend dem Umfang und anfallenden Aufgaben über ein Mindestmaß an Datenschutz-Expertise verfügen.

Wie bereits erwähnt, nimmt die Geschäftsrolle insbesondere bei der Erarbeitung der Datenschutz-Strategie eine tragende Rolle ein. Zudem werden diese in regelmäßigen Zeitabständen, z.B. halbjährig über den Ist-Zustand des Datenschutzes informiert und bei sensiblen Angelegenheiten wie bspw. die Meldung eines Datenschutzverstoßes an die Datenschutzaufsichtsbehörde oder an die Betroffenen involviert.

Für die Erarbeitung und Manifestation der Datenschutz-Strategie wird das sog. Datenschutz-Council einberufen. Ein Datenschutz-Council besteht in der Regel aus dem Datenschutzbeauftragten, der Informationssicherheit (CISO), der Rechtsabteilung und ggf. weiteren Abteilungen wie bspw. Data Governance. Dieses bricht die Datenschutz-Strategie in konkrete Richtlinien herunter, die jedoch stärker auf die einzelnen Abteilungen und das operative Tagesgeschäft abgestimmt sind. Diese Richtlinien werden sodann in dezidierte Handlungsanweisungen übersetzt und den Datenschutzkoordinatoren vorgelegt. Für dieses Gremium wird grundsätzlich eine Geschäftsordnung vereinbart, in der die Rollen, Verantwortlichkeiten, Aufgaben und Regelungen zu den Sitzungen enthalten sind.

Überdies sieht man für die Verpflichtung der Mitarbeiter zum Datenschutz sog. Verpflichtungserklärungen vor, die die Umsetzung des Datenschutzes gewährleisten sollen.[256]

Mit Hinblick auf die Entwicklung und Implementierung der Datenschutz-Strategie im Lichte einer ESG-Strategie kann es sinnvoll sein, eine Taskforce einzurichten, die die Schnittstelle Datenschutz und ESG bedient. Auf diese Weise ist es möglich, Datenschutz als Baustein der ESG-Materie zu integrieren und dadurch Marketingvorteile zu generieren. Langfristig ist es daher ratsam, innerhalb der ESG-Organisation den Datenschutzbeauftragten oder einen Datenschutz-Experten zu involvieren, der nicht nur projektbezogen hinsichtlich der Umsetzung der Datenschutz-Strategie unterstützt, sondern auch nachhaltigen Datenschutz im ESG-Framework betreibt. So ist der in folgenden Abbildung aufgezeigte schematische Aufbau auf den Umstand hin anzupassen, dass der Datenschutz-Council um einen ESG-Experten ergänzt wird, der die Auswirkungen eines nachhaltigen Datenschutzes auf den Unternehmenserfolg und damit den ESG-Score abschätzen kann.

[256] Vgl. *Deloitte (Hrsg.)*, Datenschutz-Organisation.

Dieser kann entweder regelmäßig in das Strategiegeschehen oder bei konkreten Fragestellungen einbezogen werden. So kann gewährleistet werden, dass der Datenschutz im Einklang mit der ESG-Strategie steht und auch als ein ESG-Bestandteil im Unternehmen wahrgenommen wird.

Abbildung 21: Schematischer Aufbau des Datenschutz-Councils mit Bedienung der Schnittstelle ESG.

Erweitere Darstellung in Anlehnung an: Deloitte (Hrsg.), Datenschutz-Organisation.

3.3.2 Aufbau eines Datenschutzmanagementsystems

Das Datenschutzmanagementsystem stellt in der Umsetzung der Datenschutz-Strategie einen elementaren Bestandteil dar. Da die Pflicht zur Etablierung eines Datenschutzmanagementsystems (im Folgenden „DSMS“) nicht ausdrücklich in der DSGVO verankert ist[257], erscheint es vor dem Hintergrund der Datenschutz-Strategie und des ESG-Scores als besonders sinnvoll ein solches zu integrieren. Zudem lassen sich die Anforderungen und Pflichten, die sich aus der DSGVO ergeben, nachweisbar umsetzen (Grundsatz der Rechenschaftspflicht). Am wichtigsten ist jedoch, dass das DSMS den Datenschutz im gesamten Unternehmen sicherstellt. Die Aufgabe eines DSMS besteht darin, betreffende Dokumente für den Datenschutz zu erstellen, zu verbessern und systematisch weiterzuentwickeln.[258] Darüber hinaus ist das DSMS in die Aufbau- und Ablauforganisation des Verantwortlichen einzubetten. Dieses sollte auf die Unternehmensstruktur und -organisation unter Berücksichtigung aller Standorte, auch in Drittländern und Geschäftsmodelle abgestimmt werden. Zudem sind darin auch alle Datenflüsse und datenschutzrechtliche Besonderheiten wie etwa die Verarbeitung von besonderen personenbezogenen Daten, Anzahl automatisierter Einzelfallentscheidungen enthalten.[259] Ein weiterer wichtiger Bestandteil des DSMS ist ferner die Überprüfung, Bewertung und Evaluierung der TOM sowie die damit zusammenhängenden Schutzziele Privacy by Design und Privacy by Default. Zwingende Inhalte eines DSMS sind daher:

[257] Vgl. *Schmidt*, in: Beck'sches Rechtsanwalts-Handbuch, Teil B § 50 XII 2., Rn. 109.
[258] *Schmidt*, in: Beck'sches Rechtsanwalts-Handbuch, Teil B § 50 XII 2., Rn. 109.
[259] *Schmidt*, in: Beck'sches Rechtsanwalts-Handbuch, Teil B § 50 XII 2., Rn. 109.

- Definition der Datenschutz-Ziele
- Definition einer datenschutzrechtlichen Selbstverpflichtung (Code of Privacy Conduct)[260]
- Festlegung der Datenschutzrichtlinie
- Prozessdefinition von Verarbeitungsvorgängen, bei denen personenbezogene Daten verarbeitet werden
- Prozesse zur Sicherstellung der Betroffenenrechte
- Prozesse zur Handhabung von Datenschutzverletzungen
- Prozess zur Analyse der allgemeinen Datenschutzrisiken

3.3.3 Kommunikation der Datenschutz-Strategie

Eine Datenschutz-Strategie kann allein mit einer Datenschutzorganisation nicht effektiv umgesetzt werden. Vielmehr müssen alle Stakeholder aber insbesondere jeder einzelne Mitarbeiter über die Existenz einer Datenschutz-Strategie informiert und zur Umsetzung animiert werden.[261] Dies gelingt nur durch eine adäquate Kommunikation innerhalb des Unternehmens. Die Herausforderung liegt jedoch in der Menge, Häufigkeit sowie Art und Form der Information, die an die Mitarbeiter übermittelt werden sollen. Denn eine zu intensive Kommunikation führt häufig zu einer Informationsüberflutung und damit zu einer Ablehnung seitens der Mitarbeiter führen. D.h., es sollten nicht nur ausschließlich allgemeine Informationen über die Datenschutz-Strategie kommuniziert werden, sondern es ist ratsam, die Informationen unter den folgenden Gesichtspunkten zu übermitteln:

1. Wer braucht welche Informationen, um Effektivität zu gewährleisten?
2. Wer steuert die Kommunikation und ist für diese verantwortlich?
3. Welche Medien sind in welchem Rhythmus zu benutzen? Z.B. Intranet, Flugblätter etc.
4. Wie adressatenfreundlich sind die Informationen?
5. Welche Konsequenzen gibt es, wenn nicht informiert wird?
6. Welche Interessen haben die Abteilungen und weitere Stakeholder an der Umsetzung der Strategie?
7. Wo bestehen Abhängigkeiten? Wo könnten sich Kollisionen oder Interdependenzen im Unternehmen ergeben?

Ein besonderes Augenmerk ist während der Umsetzung stets auf die Interessen der Stakeholder und dessen Einflussnahme auf die Umsetzung zu legen. Die Frage, die es hierbei zu beantworten gilt, ist, welchen konstruktiven Beitrag eine Stakeholder-Gruppe zur Strategieumsetzung beitragen kann. Um eine adressatengerechte Kommunikation durchzuführen, ist basierend auf den oben genannten Fragen und Antworten eine Kommunikationsmatrix zu erstellen. In dieser sind interne und externe Zielgruppen zu definieren, Ziele und Inhalte der Kommunikation, die dazu gehörenden Gremien und das gewählte Medium zu definieren. Daneben sind auch der Rhythmus und die verantwortliche Person aufzunehmen.

3.4 5. Schritt: Überprüfung der Datenschutz-Strategie

Bei dem Prozess der Strategieerarbeitung handelt es sich um einen kontinuierlichen Prozess, der sein Ende nicht mit der Umsetzung der Datenschutz-Strategie findet. Vielmehr muss eine Strategie überprüft und überarbeitet werden, um diese an dem wandelnden

[260] Vgl. *Schmidt*, in: Beck'sches Rechtsanwalts-Handbuch, Teil B § 50 XII 2., Rn. 109.
[261] Vgl. *Stöger*, Strategieentwicklung für die Praxis, S. 235.

Umfeld des Unternehmens stets anpassen zu können. Sinn und Zweck der Strategieüberprüfung ist es daher, den Umsetzungsprozess zu begleiten und die Strategie weiterzuentwickeln. Hierzu werden die einzelnen Schritte zur Erarbeitung und Umsetzung einer Strategie geprüft und nachjustiert. Diesem Prozessschritt sind somit vier Fragestellungen zugrunde zu legen: Die elementare Frage, die im ersten Schritt zu untersuchen ist, ist, ob sich die erarbeiteten Inhalte, Annahmen, Aussagen und Schlussfolgerungen geändert haben. Wird diese Frage bejahend beantwortet und werden grundsätzliche Änderungen entdeckt, dann ist die Strategie oder Teile davon zu überarbeiten.[262] Ferner ist als zweitens zu klären, ob sich seit der Umsetzung der Strategie neue Chancen oder Maßnahmen ergeben haben. D.h. während der Überprüfung oder erneuter Anwendung der Strategieinstrumente kommt es bei einem dynamischen Umfeld häufig dazu, dass neue Themen an Strategierelevanz gewinnen und daher mit in die Strategie einbezogen werden müssen. Auf der operativen Ebene ist daraufhin zu klären, inwiefern die festgesetzten Ziele und Maßnahmen erreicht wurden und prüft damit den aktuellen Stand. Hierzu werden quantitative Kennziffern herangezogen, Ressourcen und Maßnahmen in Prüfung gestellt. Basierend auf den Erkenntnissen aus den Fragen 1-3 wird sodann erfragt, welche Teile, Maßnahmen und Ziele der Strategie nachjustiert und wo neue Schlüsselentscheide gefällt werden müssen. Hierdurch können neue Ressourcen und Mittel festgesetzt sowie neue Stoßrichtungen definiert werden. Es ist ratsam eine jährliche Strategieüberprüfung durchzuführen, um dadurch eine flexible und robuste Datenschutz-Strategie aufrechtzuerhalten. Mit dem Ende der Strategieüberprüfung beginnt somit die Weiterentwicklung und damit wieder der Strategiekreislauf von Abbildung 14 von erneut. Für eine wirksame Strategieüberprüfung kann der Einsatz eines Strategieberichts helfen. In solch einem Strategiebericht werden die wichtigsten Aspekte der Umsetzung und Weiterentwicklung zusammengefasst. So bspw. den Ist-Zustand der Strategieerreichung, welche Maßnahmen sind die nächsten Monate zur Umsetzung der Strategie erforderlich, wo sind Schlüsselentscheidungen erforderlich und welche Bereiche der Strategie anzupassen sind.[263]

4 Datenschutzrisikomanagement im ESG-Framework als Teil der Strategieumsetzung

Für Unternehmen, die von Datenschutzrisiken bedroht sind, erweist sich ein Risikomanagement als unerlässlich. Insbesondere im Rahmen der Strategieumsetzung gilt es Risiken adäquat zu behandeln und die erfolgreiche Umsetzung der Datenschutz-Strategie sicherzustellen. Unter „Risiko“ wird allgemein die Möglichkeit einer negativen Divergenz eines tatsächlichen Ergebnisses von einem erwarteten Ergebnis (i.S. einer Verlust- oder Schadensgefahr) verstanden.[264] Für das Datenschutzrisikomanagement kann jedoch auf die Risikodefinition aus der Informationssicherheit abgestellt werden. Dieser definiert Risiken als eine „Möglichkeit, dass eine vorhandene Bedrohung eine Schwachstelle eines Wertes oder einer Gruppe von Werten ausnutzt und dadurch der Institution Schaden zufügen könnte“.[265] In diesem Kontext ist der Wert als personenbezogenes Datum zu verstehen, das bei einer Ausnutzung ein Schaden der Institution/dem Unternehmen droht. Risiken werden über die zwei Größen Eintrittswahrscheinlichkeit und Schadensausmaß

[262] Vgl. *Stöger*, Strategieentwicklung für die Praxis, S. 239.
[263] Vgl. *Stöger*, Strategieentwicklung für die Praxis, S. 235 ff.
[264] Vgl. *Gleißner/Füser*, Praxishandbuch Rating und Finanzierung, S. 33.
[265] Definition des Risikobegriffs stammt aus der ISO 27000.

ausgedrückt. [266] Ein gutes Datenschutzrisikomanagement ermöglicht es Unternehmen, den eigenen Risk Exposure Score zu senken und den Risk Management Score zu erhöhen. Auf diese Weise können diese autonom den ESG-Score, das Anlageverhalten der Investoren und den Zugang zum Kapitalmarkt positiv beeinflussen. Ein Risikomanagementprozess wird zur Analyse, Bewertung von Risiken und Definition von risikobehandelnden Maßnahmen eingesetzt. Mittels eines Risikomanagements wird das Unternehmen in die Lage versetzt, die eigenen Verarbeitungsvorgänge besser zu verstehen und anzugehen. Unternehmen fehlt es hierbei oftmals an der notwendigen Expertise und Erfahrung, solch ein Datenschutzrisikomanagementprozess eigenständig zu definieren und zu durchlaufen. Vor allem bei einer Betriebsblindheit, die zur Nichterkennung von Risiken führen kann, ist es sinnvoll einen externen Dritten in das Geschehen zu involvieren. Daher liegt es oft in der Aufgabe von Unternehmensberatern, ein adäquates Risikomanagement hinsichtlich Datenschutzrisiken aufzusetzen. Berater stehen daher vor der Herausforderung die Datenschutzrisiken zu analysieren, zu bewerten und zu steuern.

Zwar verfolgt die DSGVO mit der Datenschutz-Folgenabschätzung in Art. 35 einen risikobasierten Ansatz, jedoch betrachtet dieser lediglich die Risiken für die Rechte und Freiheiten der betroffenen Personen.[267] Risiken, die sich für Unternehmen durch die Sensibilität der Verarbeitungsvorgänge oder Ähnliches ergeben, werden nahezu vollkommen außer Betracht gelassen. Eine Anforderung zur Durchführung einer Risikoanalyse und -bewertung für die sich hieraus ergebenden Risiken für Unternehmen existiert nicht analog zum Aktiengesetz und Gesetz betreffend die Gesellschaft mit beschränkter Haftung. Für die Verantwortlichen ergibt sich lediglich die Pflicht zur Definition technisch und organisatorischer Maßnahmen, die dem Stand der Technik entsprechen, Art. 32 Abs. 1 DSGVO. In Ermangelung weitere Handlungsempfehlungen oder Leitlinien ist es notwendig, einen Risikomanagementansatz zu definieren, der die Risiken aus der DSGVO für die Unternehmen als Risiko-Objekt begutachtet.

4.1 Prozess des Datenschutzrisikomanagements

Der Prozess des Datenschutzrisikomanagements wird dabei in Anlehnung des Risikomanagements aus der IT-Sicherheit gestaltet. Grundsätzlich besteht die Aufgabe des Risikomanagements in der Existenzsicherung sowie der Erreichung der Unternehmensziele (Zukunftssicherung) unter Berücksichtigung leistungswirtschaftlicher, finanzieller und sozialer Aspekte. Im Rahmen dessen sind dabei folgende Fragestellungen zu beantworten[268]:

1. Welchen Datenschutzrisiken ist das Unternehmen in Zukunft ausgesetzt?
2. Welche Auswirkungen können die Risiken kurz- und langfristig haben?
3. Wie ist mit den Risiken umzugehen?
4. In welcher Weise können vorhandene oder entstehende Risiken vermieden oder begrenzt werden?

[266] Vgl. *Loomans/Matz/Wiedemann*, Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, S. 97.
[267] Vgl. *Hubard/Seiersen*, How to Measure Anything in Cyber Security Risk, S. 36.
[268] Vgl. *Bitkom (Hrsg.)*, IT-Risiko und Chancenmanagement im Unternehmen, S. 9.

Daher unterteilt sich der Datenschutzrisikomanagementprozess in vier Phasen und ist kontinuierlicher Natur, der in einem regelmäßigen Turnus zu durchlaufen ist:[269]

- Risikoidentifikation: Diese Phase beinhaltet die strukturierte und kontinuierliche Ermittlung aller wesentlichen Risiken bzw. Risikobereiche.
- Risikoanalyse- und bewertung: Risiken, die im vorherigen Schritt ermittelt wurden, werden mithilfe von Größen analysiert und anschließend bewertet.
- Risikobehandlung: Für die eruierten Risiken werden im darauffolgenden Schritt Risikobehandlungsmaßnahmen definiert.
- Risikoüberwachung: Sowohl die Risiken als auch die ergriffenen Maßnahmen müssen einer regelmäßigen Prüfung unterliegen.

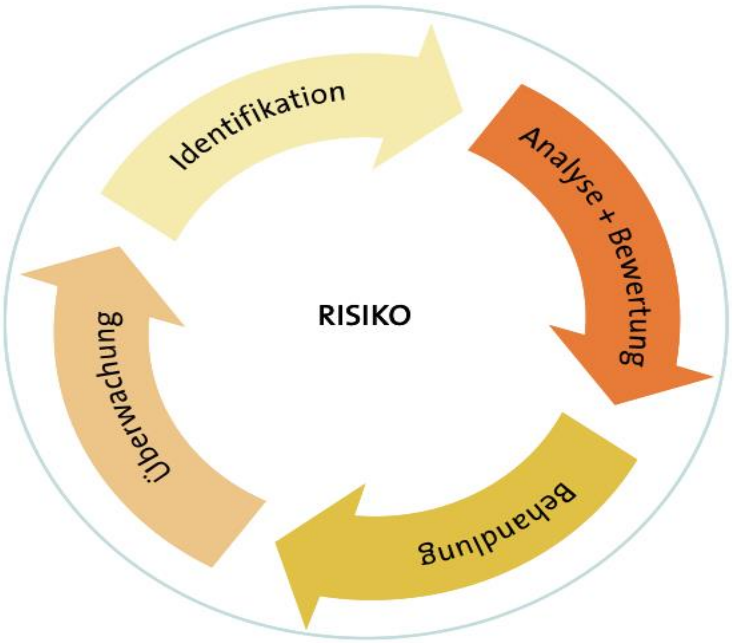

Abbildung 22: Prozess des IT-RCM. Bitkom (Hrsg.), S. 18, online abrufbar unter: https://www.bitkom.org/sites/default/files/file/import/060601-Bitkom-Leitfaden-IT-Risikomanagement-V10-final.pdf, zuletzt besucht am 28.09.2022.

4.2 RISIKOIDENTIFIKATION

Im ersten Schritt erfolgt die Identifizierung der Risiken.[270] In dieser Phase werden strukturiert und kontinuierlich alle wesentlichen Datenschutzrisiken ermittelt. Es werden alle Risi-

[269] Vgl. u.a. *Loomans/Matz/Wiedemann*, Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, S. 93 ff.; *Bitkom (Hrsg.)*, IT-Risiko und Chancenmanagement im Unternehmen, S. 16 ff.

[270] Vgl. u.a. *Loomans/Matz/Wiedemann*, Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, S. 97.; *Bitkom (Hrsg.)*, IT-Risiko und Chancenmanagement im Unternehmen, S. 20.

ken eruiert, die eine Auswirkung auf die Erreichung der Unternehmensziele haben, um daraufhin den Grad der Auswirkung, die Interdependenzen zu anderen Risiken und die Wechselwirkung auf die Geschäftsprozesse zu ermitteln.[271] Damit externe Berater eine gesamte Übersicht über das Unternehmen erhalten, ist es notwendig, die Unternehmensleitung in die Identifikation von Datenschutzrisiken einzubeziehen und insbesondere in dieser Phase das Top-Dow-Verfahren heranzuziehen. Von hoher Bedeutung ist es zudem, dass hierbei alle Unternehmensbereiche und -prozesse involviert werden. Vorerst sind die Risikoobjekte innerhalb des Unternehmens zu identifizieren – die in diesem Zusammenhang die personenbezogenen Daten darstellen.[272] Hierzu bieten sich insbesondere Workshops mit den Mitarbeitern des Kunden und der Unternehmensleitung an, in dem gemeinsam anhand einer bestehenden Risikosystematik, potentielle Risiken für die Unternehmensziele und den Unternehmenserfolg abgeleitet werden.[273] Auch die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO oder das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO stellen Instrumente dar, die zur rudimentären Erfassung der Risiken eingesetzt werden können. Die Risikosystematik kann sich nach den Kategorien der personenbezogenen Daten, den Geschäftsprozessen, Geschäftsbereichen oder den Rechtsgrundlagen nach denen sie erhoben werden orientieren. Die ermittelten Risiken werden sodann in einem Risikoregister verzeichnet, das kontinuierlich um neue Risiken aktualisiert wird und als Fundament für die anschließende Risikoanalyse dient.[274] Da Geschäftsprozesse einer Dynamik unterliegen und demzufolge auch neue Verarbeitungsvorgänge etabliert werden, sollte die Aufnahme neuer Verarbeitungsvorgänge unmittelbar außerhalb des Verzeichnisses der Verarbeitungstätigkeiten erfasst werden, bspw. über ein Formular, welches durch das betroffene Geschäftsbereich auszufüllen ist. Dieses ist sodann in das bestehende Risikoregister aufzunehmen. Dabei kann zwischen folgenden Risiken differenziert werden:

1. Wirtschaftliche und rechtliche Risiken:[275] Hierbei handelt es sich um Risiken, die rechtliche und finanzielle Konsequenzen nach sich ziehen. Hierbei sieht die DSGVO zum einen empfindliche Bußgelder nach Art. 83 DSGVO vor, zum anderen sind jedoch auch die von dem Datenschutzverstoß tangierten Personen zur Geltendmachung von Schadenersatzansprüchen befugt, Art. 82 DSGVO. Diese bergen insbesondere daher ein hohes Risiko, da die Gerichte die Kriterien der Bußgeldberechnung der Berechnung der Schadenersatzsumme zugrundlegen.[276] Im Übrigen sind seit dem 01.12.2021 Telemedienanbieter von den Vorschriften des Telekommunikation-Telemedien-Datenschutzgesetzes[277] (im Folgenden „TTDSG“) betroffen. Hiernach sind neben den Bußgeldern auch Freiheitsstrafen bei einem Verstoß gegen das Fernmeldegeheimnis vorgesehen, §§ 27 und 28 TTDSG.

2. Prozessuale Risiken: Ferner gehen Risiken auch von den Prozessen als solches aus, da unternehmesinterne Prozesse im Lichte des Datenschutzes ausgestaltet werden müs-

[271] Vgl. *Bitkom (Hrsg.)*, IT-Risiko und Chancenmanagement im Unternehmen, S. 20.
[272] *Loomans/Matz/Wiedemann*, Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, S. 97.
[273] Vgl. *Bitkom (Hrsg.)*, IT-Risiko und Chancenmanagement im Unternehmen, S. 20.
[274] Vgl. u.a. *Loomans/Matz/Wiedemann*, Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, S. 97 ff.
[275] In Anlehnung an *Bitkom (Hrsg.)*, IT-Risiko und Chancenmanagement im Unternehmen, S. 19.
[276] Vgl. u.a. OLG Frankfurt a.M., Urteil vom 14.4.2022 – 3 U 21/20, BKR, 534, 539, Rn. 51; LG Lüneburg, Urteil vom 14.7.2020 – 9 O 145/19, BKR, 306, 308, Rn. 51.
[277] Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutz-Gesetz, im Folgenden: TTDSG) vom 01.12.2021.

sen. Ein Risiko kann sich bspw. dann ergeben, wenn der Prozess zur Beantwortung von Betroffenenanfragen nicht adäquat ausgestaltet ist und hierdurch den Anfragen nicht nachgekommen werden kann. Oder aber auch, wenn bei der Bestellung über den Online-Shop des Verantwortlichen, die Einwilligung nicht integriert ist, oder datenschutzrechtliche Defizite aufweist und folglich keine wirksame Einwilligung eingeholt wurde.

3. Organisatorische und technische Risiken: Denkbar sind organisatorische Risiken, wenn kein geeignetes Berechtigungskonzept definiert ist und somit jeder beliebige Beschäftigte Zugriff auf personenbezogene Daten hat, ohne Beachtung des Need-to-Know-Prinzips. Die in den Security-Policies dokumentierten IT-Sicherheitsmaßnahmen wie Passwortvergabe, Datensicherung etc. werden in den Unternehmen teilweise missachtet, so dass personenbezogene Daten für jedermann zugänglich sind. Auch wirkt sich das fehlende Risikobewusstsein negativ auf solche Missstände aus, wodurch Workshops und regelmäßige Sensibilisierungsmaßnahmen unabdingbar sind.[278] Ferner kann das Risikoniveau erheblich steigen, wenn die Datenschutzabteilung ausschließlich zentral geführt wird, in den einzelnen Fachbereichen keine Ansprechperson für datenschutzrechtliche Fragestellungen zu finden sind (z.B. Datenschutzkoordinator) und zusätzlich die Sensibilität der Mitarbeiter für den Datenschutz nicht stetig geschult wird. Auch eine fehlende oder misslungene Pseudonymisierung stellt ein technisches Risiko für den Verantwortlichen dar.

4. Dienstleisterbezogene Risiken: Datenschutzspezifische Risiken können jedoch auch in der Beziehung zu Dienstleistern aufleben. Findet bspw. eine Datenübermittlung durch einen Dienstleister an einen Subdienstleister mit Sitz in einem unsicheren Drittland ohne angemessene Standardvertragsklauseln statt, so kann dies zur erhöhten Berechnung von Bußgeldern oder Schadensersatzansprüchen führen. Zudem verursacht eine Missachtung oder Nichtumsetzung der vereinbarten technischen und organisatorischen Maßnahmen eine Erhöhung des Risikos, insofern der Verantwortliche keine regelmäßige Überwachung zur Überprüfung der TOM durchgeführt hat.

4.3 RISIKOANALYSE UND -BEWERTUNG

Die Risikoidentifizierung und das damit zusammenhängende Risikoregister ebnet den Weg für die zweite Phase des Datenschutzrisikomanagementprozesses, womit die Analyse und Bewertung der ermittelten Risiken beginnen. Im Rahmen der Risikoanalyse werden Kriterien sowie die Risikoquelle, betroffene personenbezogene Daten, Bedrohungen, Schwachstellen und mögliche Auswirkungen analysiert.[279] Als Ergänzung kann die Prozessanalyse durchgeführt werden. Die Prozessanalyse zeigt datenschutzrechtliche Schwachstellen in den einzelnen Prozessschritten auf, um diese im Anschluss adäquat schließen zu können.[280] Die Risikobewertung hingegen umfasst die Analyse der Risikoursachen (Risikofaktoren), die Quantifizierung der Auswirkungen von Risiken auf die finanziellen und nicht-finanziellen Unternehmensziele sowie die Einschätzung der Relevanz des Risikos.[281] Das Risiko wird anhand den Messgrößen Eintrittswahrscheinlichkeit und dem potenziellen Schadensausmaß dargestellt. Außerdem gehört die Aggregation von Einzelrisiken zum Gesamtrisiko zur Risikobewertung eines Unternehmens. Für den Begriff der Risikobewertung existiert allerdings keine einheitliche Definition, wodurch die Begriffe

[278] Vgl. *Bitkom (Hrsg.)*, IT-Risiko und Chancenmanagement im Unternehmen, S. 19.
[279] Vgl. *Bitkom (Hrsg.)*, Risk Assessment & Datenschutz-Folgenabschätzung, S. 26.
[280] Vgl. *Loomans/Matz/Wiedemann*, Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, S. 112 ff.
[281] *Vgl. Burger/Buchhart*, Risikocontrolling, S. 101.

Risikomessung, Risikoquantifizierung, Risikoanalyse und Risikobeurteilung synonym verwendet werden. Zu unterstreichen ist dabei, dass die Risikobewertung nicht nur zur Orientierung für Investitionsentscheidung beiträgt, sondern einen elementaren Bestandteil für Entscheidungen und zur Steuerung der Risiken auf der Führungsebene darstellt. Die Bewertung der Risiken der Informationssicherheit lässt sich auch auf die Evaluierung datenschutzspezifischer Risiken analog anwenden. Parameter dieser Risikobewertung sind die Eintrittswahrscheinlichkeit des Risikos und die Schadenshöhe als unsichere Ereignisse.[282]

Die Schäden können dabei unterschiedliche Ausprägungen haben:[283]

- Der Betroffene selbst wird durch einen Datenschutzvorfall geschädigt.
- Das Unternehmen erleidet einen Vermögensschaden, z.B. ein Bußgeld.
- Das Unternehmen erleidet einen Nichtvermögensschaden, z.B. Reputationsschäden.

Die Schadenshöhe lässt sich neben der Szenarien-Methode, bei der realitätsnahe Szenarien durchlaufen werden, insbesondere für wirtschaftliche und rechtliche Risiken auch anhand der bisher erteilten Bußgelder und Gerichtsurteilte teilweise bestimmen. Den Unternehmensberatern ist zu daher zu raten, eine aktuelle Übersicht über die bisher ausgesprochenen Bußgelder sowie Schadensersatzsummen zu erstellen, die auf den Sektor, auf die Rechtsgrundlagen der Verarbeitungsvorgänge oder auf diese selbst des jeweiligen Unternehmens zutreffen.[284] Daraufhin können gegebenenfalls Summenbereiche für die betroffenen Risiken definiert werden.

Im nächsten Schritt ist die zweite Ausprägung der Risikobewertung – und zwar die Eintrittswahrscheinlichkeit zu ermitteln. Dies mag sich in der Praxis etwas schwieriger gestalten als die Ermittlung der Schadenshöhe, da diese auch durch die subjektive Einschätzung beeinflusst wird. Die Eintrittswahrscheinlichkeit wird durch 3 Faktoren (Bedrohungen, Schwachstellen sowie technische und organisatorische Maßnahmen) determiniert:[285]

1. Bedrohungen: Im Unternehmen können durch sog. Bedrohungen Schäden entstehen und kann dabei parallel auf mehrere Risikoobjekte (personenbezogene Daten) einwirken. In Anlehnung an die ISO 27005 und Annex C, lassen sich folgende Bedrohungen klassifizieren:

- Menschliches Fehlverhalten
- Externe Angriffe
- Technische Fehlfunktionen

Hierfür wird jedoch vorausgesetzt, dass die Bedrohung vorhandene Schwachstellen ausnutzt.

2. Schwachstellen: Wie bereits erwähnt, dienen Schwachstellen der Ausnutzung durch Bedrohungen und sind kausal ursächlich für Schäden, die dem betroffenen Unternehmen entstehen. Folgende Schwachstellen können ausgenutzt werden:

---

[282] Vgl. *RMA Risk Management & Rating Association e.V. (Hrsg.)*, Risikoquantifizierung, S. 29.
[283] Vgl. *Loomans/Matz/Wiedemann*, Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, S. 98.
[284] Siehe hier auch eine Auflistung aller ausgehängten Bußgelder unter: https://www.enforcementtracker.com.
[285] Vgl. *Loomans/Matz/Wiedemann*, Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, S. 98.

- Das Geschäftsmodell im Zusammenhang mit dem untersuchten Risikoobjekt (Marketing vs. F&E), mit Hinblick auf die Ermittlung des MSCI ESG-Ratings scheint dieses als eine bedeutende Schwachstelle, da diese die Key Issue Score auf Grundlage des Global Industry Classification Standards ermittelt.
- Welche **Systeme** werden eingesetzt? Dem Überblick dienend kann die Systemlandschaft zur Identifizierung herangezogen werden.
- Existieren standortbezogene Schwachstellen? Wenn ja, welche? Ist die Besucherfrequenz des Gebäudes hoch oder handelt es sich eher um ein kontrolliertes Rechenzentrum?
- Werden Dienstleister eingesetzt? Wenn ja, welche? An der Stelle können Schwachstellen insbesondere im Vertragswerk als auch in der Datenübertragung identifiziert werden.
- Die größte Schwachstelle eines Unternehmens ist der Mensch selbst.

3. Technische und organisatorische Maßnahmen: Es ist jedoch nicht so, dass die Unternehmen den Schwachstellen und Bedrohungen hilflos ausgeliefert sind. Vielmehr können diese technische und organisatorische Maßnahmen ergreifen, um diese Schwachstellen vorab zu minimieren. Diese sind auch Bestandteil des folgenden Prozessschrittes der Risikobehandlung. Eine Reduktion der Schwachstellen auf 0 ist jedoch allein aus wirtschaftlichen Gesichtspunkten nicht sinnvoll und auch nicht möglich. An der Stelle ist durch die Unternehmensberater zusammen mit dem Kunden gewiss zwischen dem Schutzzweck und dem vertretbaren Aufwand der TOMs abzuwägen. Die TOMs stellen damit das aufwändigste und letzte Kriterium der Ermittlung der Eintrittswahrscheinlichkeit dar.

Alle drei der oben benannten Faktoren sind demnach bei der Ermittlung der Eintrittswahrscheinlichkeit in Erwägung zu ziehen. Die Herausforderung besteht im nächsten Schritt jedoch in der Auswahl der Risikobewertungsmethodik. Dabei wird zwischen der quantitativen und der qualitativen Risikobewertung unterschieden.[286] Die qualitative Risikobewertung teilt Risiken in Risikoklassen ein, wie etwa Eintrittswahrscheinlichkeit/Schadenshöhe niedrig, mittel und hoch.[287] Bei der quantitativen Risikobewertung werden die Risiken in der Regel mithilfe eines monetären Wertes oder einer Kennziffer als Ausdruck für die Schadenshöhe und Eintrittswahrscheinlichkeit beschrieben. Allerdings lassen sich nicht alle ESG-Risiken in monetären Werten beziffern. Insbesondere Risiken mit Bezug zu ESG sind eher immaterieller Natur und beziehen sich nicht ausschließlich auf nicht-monetäre Ziele wie z.B. die Senkung der Schadstoffemissionen in der Produktion. Der quantitative Ansatz liefert zwar exakte Key Performance Indikatoren, allerdings setzt diese eine fundierte Informationsgrundlage voraus, um sowohl der Eintrittswahrscheinlichkeit als auch der Schadenshöhe einen monetären Wert beimessen zu können.[288] Zumindest fehlt es in diesem Kontext ausreichend an sicheren und konstanten Daten zur Ermittlung der Eintrittswahrscheinlichkeit. Auch die Berechnung einer konkreten Schadenshöhe erweist sich aktuell noch als herausfordernd, da es aufgrund strittiger Auffassungen bzgl. des Ausmaßes des Schadenersatzanspruches nach Art. 82 DSGVO noch keine dezidierten und konsistenten monetären Werte existieren.[289] In Ermangelung einer geeigneten Informationsgrundlage ist daher der qualitative Ansatz zur Berechnung der Datenschutzrisiken heran-

[286] Vgl. *Klipper*, Information Security Risk Management, S. 36.
[287] Vgl. *Loomans/Matz/Wiedemann*, Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, S. 103.
[288] Vgl. *Vanini*, Risikomanagement Grundlagen – Instrumente – Unternehmenspraxis, S. 231.
[289] Vgl. *Bitkom (Hrsg.)*, IT-Risiko und Chancenmanagement im Unternehmen, S. 20.

zuziehen. Für diese Arbeit und die Ermittlung der Schadenshöhe kann es jedoch zielführend sein, auf historische Daten, wie etwa die bisher erteilten Bußgelder oder bereits ausgesprochene Schadensersatzansprüche zurückzugreifen. Diese sind jedoch aus bereits genanntem Grund mit Vorsicht zu genießen und dienen lediglich zur Orientierung, da sowohl die Bußgelder als auch die Schadenersatzsummen noch nicht nach harmonisierten Kriterien ausgesprochen werden. Demnach kann das Niveau der Datenschutzrisiken ausgedrückt werden als Eintrittswahrscheinlichkeit multipliziert mit der Schadenshöhe. So können Datenschutzrisiken anhand der bekannten Risikomatrix priorisiert und dargestellt werden. Exemplarisch lässt sich folgende Risikomatrix für ein Technologieunternehmen mit knapp 260 Milliarden Euro Umsatz und Sitz in den USA ermitteln.

Schadenshöhe in Euro					
	5-10 Milliarden				
	1-4 Milliarden				
	50-990 Milionen				
	1-49 Millionen				
		unwahrscheinlich	gelegentlich	wahrscheinlich	regelmäßig
		Eintrittswahrscheinlichkeit			

Abbildung 23: Risikomatrix.

Eigene Darstellung in Anlehnung an: Loomans/Matz/Wiedemann, Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, S. 104.

4.4 RISIKOBEHANDLUNG

Nachdem die identifizierten Risiken analysiert und bewertet wurden, wird die dritte Phase eingeleitet, in der dann sog. Risikobehandlungsmaßnahmen definiert werden. Hierbei unterscheidet man zwischen vier Möglichkeiten:

- Risikominimierung durch das Ergreifen von Maßnahmen hier bspw. durch den Einsatz von technischen und organisatorischen Maßnahmen,
- Risikovermeidung (bspw. durch Beendigung der Verarbeitung bestimmter Daten oder Datenkategorien),
- Risikotransfer auf Dritte (bspw. durch Outsourcing oder einer Versicherung),
- Risikoakzeptanz.

Zu beachten gilt jedoch, dass die letzteren beiden Maßnahmen auf datenschutzspezifische Risiken nur begrenzt angewendet werden können, da das Risiko nur in seltenen Fällen vollkommen auf Dritte abgewälzt oder vollkommen von einer Versicherung abgedeckt werden kann.[290] Als die gängigste und vom Gesetzgeber vorgesehene Risikobehandlung ist die Ergreifung von technischen und organisatorischen Maßnahmen. Grund-

[290] Vgl. *Bitkom (Hrsg.)*, Risk Assessment & Datenschutz-Folgenabschätzung, S. 33.

sätzlich gilt dabei, dass je höher die Eintrittswahrscheinlichkeit und die Schadenshöhe sind, umso effektivere Maßnahmen ergriffen werden müssen. Die DSGVO sieht in Art. 32 Abs. 1 vor, dass mindestens die Umsetzung der folgenden Maßnahmen geprüft werden muss:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Zudem wird in Art. 32 Abs. 4 DSGVO sowohl vom Verantwortlichen als auch Auftragsverarbeiter verlangt, dass Zugriffsbeschränkungen etabliert sind und das Need-to-Know-Prinzip gewahrt wird. Werden risikominimierende Maßnahmen ergriffen, sollte eine Maßnahmenliste geführt werden, mit den geplanten Maßnahmen, den Verantwortlichkeiten, den Risikoinhaber und die Planung, bis wann die Umsetzung abzuschließen ist. Die Maßnahmen sollten dabei stets einen präventiven Charakter haben und nicht reaktiv, sondern aktiv ergriffen werden. Hierzu bietet es sich an, sich an bereits bestehende Maßnahmenkataloge wie etwa dem IT-Grundschutz-Maßnahmenkatalog oder der ISO/IEC FDIS 29151:2016 Leitfaden für den Schutz personenbezogener Daten zu orientieren.[291]

4.5 RISIKOÜBERWACHUNG

Wie bereits beschrieben handelt es sich bei dem Datenschutzrisikomanagement nicht um einen Prozess, der mit der Definition und Umsetzung der risikominimierenden Maßnahmen sein Ende nimmt. Vielmehr sind die Risiken stets neu dem Managementprozess zu unterziehen und dieser kontinuierlich zu optimieren. Dies ist nur dann möglich, wenn die Risiken und die Maßnahmen kontinuierlich überwacht werden. Dies stellt auch den letzten und zeitgleich auch den ersten Schritt des Prozesses dar. Dem pflichtet sich auch der europäische Gesetzgeber bei und schreibt vor, dass die Wirksamkeit der technischen und organisatorischen Maßnahmen in regelmäßigen Abständen auf ihre Wirksamkeit hin überprüft werden müssen (Art. 32 Abs. 1 DSGVO). Er geht sogar noch weiter und verpflichtet die Verantwortlichen einen Prozess für interne Audits der Sicherheit der Verarbeitung zu etablieren und durchzuführen, Art. 32 Abs. 1 lit. d) DSGVO. Die Risikoüberwachung kann ebenfalls in Form von Fragebögen, Controls und Workshops unterstützt werden, indem die veränderte Risikolage sowie die Umsetzung und Effektivität der Maßnahmen abgefragt werden. In diesen ist dann ein Soll-Ist-Abgleich durchzuführen. Abweichungen bedingen, dass verbleibende oder neue Risiken durch Risikobehandlungsmethoden minimiert werden. Um der Rechenschaftspflicht nachzukommen, ist es geboten, eine ausführliche Dokumentation des Auditkonzeptes und der durchgeführten Prüfungen in Form von Audit-Berichten zu führen. Sollten in Audits Abweichungen festgestellt wer-

[291] Vgl. *Loomans/Matz/Wiedemann*, Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, S. 108; *Bitkom (Hrsg.)*, Risk Assessment & Datenschutz-Folgenabschätzung, S. 34.

den, sollte die Nachhaltung der Behebung ebenfalls systematisiert und dokumentiert werden. [292]

5 HANDLUNGSEMPFEHLUNG FÜR DIE POLITIK

Es ist unbestritten, dass nachhaltige Investoren und Anleger allein nicht ausreichen, die Materie ESG und damit inbegriffen den Datenschutz, effizient voranzutreiben. Die rasant zunehmende Klimakrise und der steigende Digitalisierungsgrad erfordern somit dringend politische Reaktionen und Maßnahmenpakete. Bisher lassen sich politische Maßnahmen nur hinsichtlich der Besteuerung von klimaeinwirkenden Geschäftstätigkeiten finden, die einen eher sanktionierenden Charakter haben. Seit Anfang 2021 gilt z.B. die CO2-Bepreisung für die Bereiche Wärme und Verkehr. Unternehmen, die mit Heizöl, Erdgas, Benzin und Diesel handeln, werden durch das Brennstoff-Emissionshandelsgesetz[293] verpflichtet, für den Treibhausgas-Ausstoß, den ihre Produkte verursachen, Emissionsrechte in Form von Zertifikaten zu erwerben.[294] Allerdings ist diese CO2-Steuer kritisch zu beäugen. Zum einen ist die Steuerlast in Deutschland ohnehin hoch. In dieser sind bereits Steuern zum Schutz der Umwelt und zur Erreichung der Klimaziele enthalten, jedoch bislang keinen großen Beitrag zur Bewältigung des Klimaproblems beigetragen haben. Überdies hat eine solche CO2-Abgabe keinen direkten Effekt und führt nicht zu einer unmittelbaren Verhinderung von Treibhausgasemissionen. Denn die CO2-Bepreisung kann als Aufpreis schlichtweg durch die Unternehmen auf die Verbraucher abgewälzt werden.[295] Eine Studie der Forscher des RWI – Leibniz Institut für Wirtschafsforschung ergab, dass zwar der Verbrauch vom Fahrer eines Benzinfahrzeuges um 0,23 Prozent gesunken ist, jedoch auf der anderen Seite mehr Benzin pro Kilometer verbraucht wird. Hierzu zogen die Forscher Daten aus den Tanktagebüchern heran, die Verbraucher für das Deutsche Mobilitätspanel geführt haben. Das RWI liegt dem die Annahme zugrunde, dass die Verbraucher angesichts der Preiserhöhung auf lange Fahrten verzichten und eher Kurzstrecken fahren. Vor diesem Hintergrund kann eine Senkung des Verbrauchs um 0,23 Prozent nicht den erhöhten Benzinverbrauch pro Kilometer kompensieren. Bei Diesel gibt es sogar weder bei der zurückgelegten Strecke noch beim Kraftstoffverbrauch Änderungen. Dies rechtfertigt damit die Aussage, dass die CO2-Bepreisung wenig bis sogar keine unmittelbare Wirkung aufzeigt.[296] Daher ist grundsätzlich zu untersuchen, wie ein politischer Pull-Effekt zur Umsetzung der Sustainable Development Goals erreicht werden kann. Ein Ansatz könnte hierbei eine steuerliche Erleichterung auf Kapitaleinkünfte sein, die auf den drei Säulen ESG basieren. Dies könnte in der Praxis so gestaltet werden, dass Einkünfte von Investoren, die nachweislich einer der drei Faktoren Environmental, Social oder Governance berücksichtigen bspw. durch einen Nachweis eines Bankinstitutes, nicht der vollen Steuerlast nach dem Einkommenssteuergesetz unterliegen, wie nicht ESG-orientierte Investitionen. Somit wird für Investoren und Anleger ein Anreiz gesetzt, diese drei Kriterien mit ihre Entscheidungsfindung zu berücksichtigen und dadurch den Anteil jener Investitionen zu erhöhen. Dies wiederum erhöht den Druck auf Unternehmen ihre Geschäftstätigkeit und Unternehmensstrategie auf die drei ESG-Elemente auszurichten, um damit den ESG-Score zu optimieren und die Entscheidungsfindung der Aktionäre und Anleger zu beeinflussen.

---

[292] Vgl. *Bitkom (Hrsg.)*, Risk Assessment & Datenschutz-Folgenabschätzung, S. 35.
[293] Brennstoffemissionshandelsgesetz vom 12. Dezember 2019 (BGBl. I S. 2728), das durch Art. 1 des Gesetzes vom 3. November 2020 (BGBl. I S. 2291) geändert wurde.
[294] Vgl. *Bundesregierung (Hrsg.)*, Anreiz für weniger CO2-Emissionen.
[295] Vgl. *Handelsgesetzblatt (Hrsg.)*, Was die CO2-Steuer für Verbraucher bedeutet.
[296] Vgl. *ZEIT ONLINE (Hrsg.)*, Als hätte man 360.000 Autos stillgelegt.

Auch für den Datenschutz lassen sich ähnlich wie für das Klimaproblem nur Sanktionen in der DSGVO wiederfinden. Trotz der empfindlichen Bußgelder geben im Jahr 2021 nur 20 Prozent der Unternehmen an, die Anforderungen der DSGVO vollständig umgesetzt und einen Prüfprozess zur Weiterentwicklung etabliert zu haben.[297] Daher scheinen die Bußgelder nur einen begrenzten Effekt zu zeigen, weshalb auch hier wieder der Bedarf für Anreize auf politischer Ebene besteht. Es sind damit politische Ansätze zu entwickeln, die eine vollständige Integration des Datenschutzes in ihre Portfolios durch die Finanzinstitute und ESG-Agenturen ermöglichen. Allerdings können Ratingagenturen und Finanzinstitute den Datenschutz erst vollumfänglich berücksichtigen, wenn Unternehmen ausreichend Informationen über die Erfüllung der DSGVO-Anforderungen der Öffentlichkeit zur Verfügung stellen. Daher wächst das Bedürfnis nach einer (gesetzlichen) Pflicht zur öffentlichen Berichterstattung der Unternehmen, welche die benötigten Informationen zum nachhaltigen Umgang mit Daten bereitstellen. Gegenstand eines solchen Berichts sind die Erklärung eines Unternehmens zu den Auswirkungen auf die Privatsphäre der Betroffenen und wie diese bewältigt werden. Ratsam wäre eine jährliche Veröffentlichung des Datenschutzberichts mit folgendem Mindestinhalt, das sich an dem GRI-Standard orientiert[298]:

1. Die gesamte Anzahl der substantiierten Datenschutzverstöße oder Beschwerden durch die Betroffenen, in zwei Kategorien gegliedert werden:

    a) Beschwerden, die von externen Dritten eingereicht werden und von dem Unternehmen verursacht worden sind

    b) Beschwerden von den Aufsichtsbehörden

2. Gesamtanzahl festgestellter Datenlecks, Datendiebstähle oder Verlust der Kundendaten

3. Ergriffene Maßnahmen (z.B. Meldung an die Betroffenen und Aufsichtsbehörden)

4. Angaben zum Datenschutzrisikomanagement und zum Datenschutzmanagementsystem sowie zur Durchführung von Audits der Dienstleister und dem Unternehmen selbst.

6 FAZIT

ESG wird insbesondere durch Klimakrisen und menschenrechtsverletzenden Arbeitsbedingungen getrieben. Jedoch lassen die drohenden Bußgelder und Sanktionen aus der DSGVO sowie die steigenden Erwartungen der Betroffenen an mehr Datenschutz keinen Raum für Missachtung dieser Anforderungen. Bereits im Volkszählungsurteil erkannten die Richter die Risiken einer massiven Datenverarbeitung ohne adäquaten Schutz für die Betroffenen an. Daher ergibt sich die Notwendigkeit, zu untersuchen, ob der Datenschutz ebenfalls ein ESG-Anliegen und wo dieses einzuordnen ist. Eine Vereinbarkeit von ESG und Datenschutz ist dann allerdings nur dann möglich, wenn man den Sinn und Zweck des Datenschutzes mit der Bedeutung der Nachhaltigkeit im Einklang steht und als solches zu definieren ist – die DSGVO lediglich als gesetzliches Konstrukt wahrzunehmen greift an dieser Stelle zu kurz. Wird der DSGVO genügend auf dessen Hintergrund untersucht und betrachtet man den Schutz der Daten als moralische Verpflichtung, die informationelle Selbstbestimmung der Betroffenen zu wahren, resultiert daraus das Ergebnis,

[297] Vgl. *Bitkom (Hrsg.)*, Datenschutz als Daueraufgabe für die Wirtschaft: DS-GVO & internationale Datentransfers, S. 2.
[298] In Anlehnung an *GRI Standards (Hrsg.)*, GRI 418: Customer Privacy 2016, S. 8.

dass es sich hierbei zweifelsohne um ein Menschenrecht handelt und Bestandteil einer Corporate Digital Responsibility ist. Die neue Verantwortung der steigenden Digitalisierung, von der insbesondere Unternehmen Profitträger sind, besteht daher in der Achtung der Datensouvernität jedes einzelnen Individuums. Die Frage, wo der Datenschutz in der ESG-Ära angesiedelt werden kann, lassen sich anhand der Historie und des Schutzzwecks der DSGVO beantworten. Die Anerkennung des Schutzes personenbezogener Daten als Grundrecht sowohl in der Grundrechtecharta als auch im deutschen Grundgesetz stützt die Einordnung des Datenschutzes in der Social-Säule, da es sich dabei auch um ein ausdrücklich normiertes und unbeschränktes[299] Menschenrecht handelt. Unternehmen müssen daher Programme und Strategien entwickeln, die nicht nur auf Datenschutz-Compliance ausgelegt sind, sondern auch positive und soziale Ziele erreichen.[300] Andererseits ist die Tatsache nicht zu verkennen, dass es zwischen den ESG-Säulen und dem Datenschutz zu Kollisionen und damit zu Zielkonflikten kommen kann. Einerseits ist darauf Acht zu geben, den ökologischen Fußabdruck und die CO2-Abgabe so weit wie möglich zu reduzieren. Andererseits ist das Risiko eines empfindlichen Bußgeldes, das aus der DSGVO hervorgeht, sowie dessen mittelbaren und nicht-monetären Risiken sorgfältig abzuwägen und in Betracht zu ziehen. Bspw. benötigen Plug-in-Hybrid-Fahrzeuge mit einem kohärenten Bonussystem zur autonomen Schaltung in den elektrischen Schaltbetrieb zumindest die Standortdaten des Fahrers, um Umweltzonen o.Ä. zu erkennen. Solch eine Maßnahme mag zwar ökologische Ziele erreichen und im Bereich Environment den Score verbessern, allerdings ist der Einsatz von Fahrzeugen mit Standorttracking datenschutzrechtlich zu würdigen und daraufhin adäquate Maßnahmen zu unternehmen, um eine datenschutzkonforme Nutzung der Fahrzeuge gewährleisten. Auch in der Social-Säule selbst können Aktivitäten mit dem Datenschutz kollidieren, wie z.B. bei der Umsetzung des Lieferantensorgfaltspflichtengesetzes, das Pflichten zur Etablierung von menschenrechtswahrenden Prozessen bereithält, die die Verarbeitung von personenbezogenen Daten beinhalten. Hieraus kann folglich die Erkenntnis gezogen werden, dass der Schutz personenbezogener Daten nicht nur als Kriterium der Social-Säule wahrzunehmen, sondern auch ein fest etablierter Bestandteil bei der Definition von Zielen im Sinne der Environment, Social oder Governance Dimension sein muss. Nachdem unbestritten festgestellt wurde, dass der Datenschutz durchaus in dem gesamten ESG-Konzept seinen Platz finden muss, ist es unentbehrlich, zu determinieren, ob Datenschutzrisiken wesentliche Auswirkungen auf die ESG-Strategie haben können. Der Wesentlichkeitsgrad eines ESG-Risikos durchläuft den sog. Materialisierungsprozess, der sich aus fünf Stadien für die Wesentlichkeit eines ESG-Risikos zusammensetzt. Mit Hinblick darauf, dass der Schutz personenbezogener Daten derweil auch in diversen anderen Gesetzen verankert ist,[301] und seit dem 25.08.2018 die DSGVO in allen Mitgliedstaaten Anwendung findet, befindet sich dieser in der Phase „Regulatory Response“ und damit im letzten Stadium des Materialisierungsprozesses. Als Ergebnis lässt sich daraus schlussfolgern, dass auch das Wesentlichkeitsmerkmal von Datenschutzrisiken eine Einbindung des Datenschutzes in das ESG-Framework befürwortet und damit zu bejahen ist.

Für Unternehmen kann es außerdem sinnvoll sein, einen Überblick über das Berechnungsmodell des ESG-Scores zu gewinnen und einen Blick auf den Status Quo der Tragweite des Datenschutzes innerhalb der Berechnungen zu werfen. Aktuell lässt sich feststellen, dass zwar Ratingagenturen derweil die Bedeutung des Datenschutzes aner-

[299] ErwGr. 14 der DSGVO gewährt jedem das Recht auf Schutz seiner personenbezogenen Daten ungeachtet der Staatsangehörigkeit oder des Aufenthaltsortes der Person.
[300] Vgl. *PWC (Hrsg.)*, Unterstützt Ihr Datenschutzprogramm Ihre ESG-Bemühungen?.
[301] Siehe u.a. Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) sowie das Bundesdatenschutzgesetz (BDSG).

kennen, jedoch nicht im gerechten Ausmaß. Bereits die fälschliche Kategorisierung in die Produkthaftung scheint der Materie nicht genügend Rechnung zu tragen; denn nicht nur auf dem Markt eingeführte Produkte sollen den Anforderungen der DSGVO genügen, sondern auch alle weiteren Services müssen Datenschutzkonformität aufweisen. Ferner verkennt der marktführende ESG-Ratingermittler MSCI ESG Rating die Tatsache, dass sich der Datenschutz nicht lediglich auf den Schutz personenbezogener Daten von Kunden und Verbraucher beschränkt, sondern auch andere Adressaten wie bspw. Arbeitnehmer oder Lieferanten umfasst. Dies ist zum Teil auch der Zuordnung zur Produkthaftung geschuldet, da hierdurch – wie bereits behandelt – suggeriert wird, dass der Datenschutz lediglich im Kundenkontext eine Tragweite hat. Schlussfolgernd bedarf es auch an dieser Stelle an einer Korrektur zum einen der Einordnung des Datenschutzes, um der Reichweite des Datenschutzes genügend Rechnung zu tragen.

Nach der vorangegangenen Analyse hat der Datenschutz zweifelsohne eine Relevanz für die ESG-Ära. Für Unternehmen besteht sodann die Herausforderung darin, den Schutz personenbezogener Daten nicht nur als Compliance-Anliegen zu verstehen, sondern diesen als freiwillige Selbstverpflichtung in der Unternehmensstrategie und ESG-Strategie im Top-Down-Verfahren zu integrieren. Der ethische und nachhaltige Umgang mit personenbezogenen Daten lässt sich vor allem durch die Entwicklung und Etablierung einer unternehmensweiten Datenschutz-Strategie ausleben. In Ermangelung eines Prozesses zur Entwicklung einer spezifischen Datenschutz-Strategie, kann hierzu der konventionelle Strategieentwicklungsprozess aus der Betriebswirtschaft herangezogen werden. Das herkömmliche Fünf-Phasen-Modell unterstützt dabei, sowohl das Unternehmen als auch das Umfeld hinsichtlich des Datenschutzes zu analysieren, um daraufhin eine adäquate Datenschutz-Strategie zu definieren und diese anschließend umzusetzen sowie zu überprüfen. Die Umfeldanalyse liefert wichtige Erkenntnisse über die Datenschutzhaltung der eigenen Zielgruppe. Anhand der GAP-Analyse werden Datenschutzdefizite innerhalb des Unternehmens identifiziert, indem man dieser die Zwecke und die Verarbeitungsvorgänge selbst, die Datenarten, Verantwortlichkeiten, bestehende Datenschutzmaßnahmen und vergangene Datenschutzverstöße zugrunde legt. Innerhalb der SWOT-Analyse werden sodann die Ergebnisse der Umfeld- und GAP-Analyse in einer höheren Granularität konsolidiert und um Chancen und Opportunitäten ergänzt. Die Ermittlung von Stärken, Schwächen, Opportunitäten und Gefahren ebnen den Weg zur Definition von strategischen Stoßrichtungen, die anschließend eine Fusionierung zur übergeordneten Datenschutz-Strategie ermöglichen. Das Fundament für eine erfolgreiche Umsetzung der Strategie in Zusammenarbeit mit der ESG- oder Nachhaltigkeitsabteilung bildet eine diverse Datenschutzorganisation und die Einberufung einer Task Force. Von erheblicher Bedeutung ist, dass in dieser nicht nur Mitarbeiter mit Datenschutzexpertise tätig sind, sondern dem auch mindestens ein Nachhaltigkeits- oder ESG-Experte beiwohnt, um so die Brücke zur ESG-Strategie zu schlagen.

Zudem lässt sich festhalten, dass die Durchführung einer Datenschutzfolgenabschätzung zu kurz greift, um den ESG-Score im Datenschutz zu optimieren. Bei der Datenschutz-Folgenabschätzung allein mangelt es nämlich an der Perspektive für die Risiken, die dem Unternehmen drohen, wodurch das Datenschutzrisikomanagement eine unabdingbare Voraussetzung für die erfolgreiche Umsetzung der Datenschutz-Strategie ist. Ziel ist es, Risiken zu identifizieren, zu analysieren sowie zu bewerten, um daraufhin Behandlungsmaßnahmen zu definieren, die im Anschluss zu überwachen sind. Unternehmen sollen damit in die Lage versetzt werden, Datenschutzrisiken rechtzeitig abzuwenden und die Unternehmensziele zu erreichen. Hierbei besteht die Herausforderung insbesondere in der Bewertung der Risiken. Da zwar die Schadenshöhe anhand der Bußgelder und der

bereits ausgesprochenen Rechtsprechung hinsichtlich der Schadensersatzansprüche aus Art. 82 DSGVO determiniert werden könnte, erweist sich die Bestimmung der Eintrittswahrscheinlichkeit als schwierig. Daher ist hier ferner auf die qualitative oder semi-qualitative Berechnungsmethode abzustellen. Zudem spielt die Ergreifung adäquater technischer und organisatorischer Maßnahmen eine federführende Rolle, da nur durch Maßnahmen, die dem aktuellen Stand entsprechen, der ESG-Score im Bereich Datenschutz optimiert werden kann. Für die Zukunft lässt sich aus den Ausführungen demnach ableiten, dass Unternehmen den Datenschutz ebenfalls als ESG-Thema wahrzunehmen haben und dahingehend ihre Prozesse und Strategien anpassen müssen. Jedoch müssen auch auf politischer Ebene weitere Handlungen folgen, um zum einen ESG im Allgemeinen und zum anderen die vollständige Integration des Datenschutzes in die Materie zu fördern. So bieten sich steuerliche Begünstigungsmodelle für ESG-Investitionen an, um die Anzahl dieser weiter zu erhöhen. Mit Hinblick auf den Datenschutz können diverse Pflichten, wie etwa eine jährliche Berichtspflicht, Unternehmen zu einer freiwilligen Selbstverpflichtung animieren.

Anlage 1: Fragebogen zur Analyse des Datenschutzumfeldes des Verantwortlichen

In diesem Fragebogen werden die Kernmerkmale der Zielgruppe zur Ausrichtung der Datenschutz-Strategie erfragt.

Frage	Antwort
Welches durchschnittliche Alter hat die Zielgruppe des Verantwortlichen?	keine Angabe
Welchen durchschnittlichen Bildungsgrad hat die Zielgruppe?	Akademischen Bildungsgrad
Wie viele Betroffenenanfragen erhält der Verantwortliche im Durchschnitt?	
Welche Normen betreffen die Betroffenenanfragen am häufigsten?	Auskunftsrecht, Art. 15 DSGVO
Führten Betroffenenanfragen in der Vergangenheit zur Eskalation an die Aufsichtsbehörde o.Ä.?	Ja
Wenn die vorherige Frage mit „Ja“ beantwortet wurde: Wie oft wurden Eskalationen ausgelöst?	
Ist die unternehmenseigene Branche vermehrt von Bußgeldern betroffen?	Ja
Wenn die vorherige Frage mit „Ja“ beantwortet wurde: Welche Normen waren am häufigsten Gegenstand dieser Bußgelder?	
Wie hoch waren die Bußgelder im Durchschnitt?	

Anlage 2: Checkliste zur Durchführung der GAP-Analyse

1. Schritt: Überblick über die bestehenden Verarbeitungsvorgänge und bestehenden Datenschutzmaßnahmen. Hierbei sollen alle Prozesse, die die Verarbeitung von personenbezogenen Daten zum Gegenstand haben, die Kategorien der Daten, internen Verantwortlichkeiten und ergriffenen technischen und organisatorischen Maßnahmen aufgelistet werden.

Vorgangs-nummer	Bezeichnung des Verarbeitungs-vorganges	Datenkatego-rien	Fach-bereich	Verant-wortliche Person	Ergriffene Tech-nische und orga-nisatorische Maßnahmen

2. Schritt: Prüfung der Datenschutzgrundsätze, des Nachkommens der Betroffenenanfragen, der datenschutzrechtlichen Verträge und der Datenübermittlung in Drittländer. In diesem Schritt wird geprüft, inwiefern die Datenschutzgrundsätze bei der Verarbeitung von personenbezogenen Daten innerhalb eines bestimmten Verarbeitungsvorganges eingehalten werden. Zu jedem einzelnen Grundsatz ist die getroffene Maßnahme anzugeben. Sollten keine Maßnahmen zu dem genannten Grundsatz vorhanden sein, so ist „keine Maßnahmen vorhanden“ anzugeben.

Vorgangsnummer:	**Bezeichnung der Verarbeitung:**

Datenschutzgrundsatz:	**Maßnahme:**
Rechtmäßigkeit	
Transparenz	
Nichtverkettung	
Datenminimierung	
Speicherbegrenzung	
Richtigkeit	
Zweckbindung	
Vertraulichkeit	

3. Schritt: Prüfung der datenschutzrechtlichen Verträge. Neben der Einhaltung der Grundsätze ist außerdem zu prüfen, ob zur Durchführung des Geschäftsprozesses auch Dienstleister eingesetzt und an diese personenbezogene Daten übermittelt werden. Wird dies bejaht, sind Verträge, die die Einhaltung der Datenschutzanforderungen sicherstellen, zu schließen und geeignete technische und organisatorische Maßnahmen zu ergreifen.

Werden zur Durchführung des Geschäftsprozesses Dienstleister eingesetzt?	Ja
Wenn ja, wurde hierzu ein Auftragsverarbeitungsvertrag geschlossen?	Ja
Besteht eine gemeinsame Verantwortlichkeit mit Dritten?	Ja
Wenn ja, wurde hierzu ein Vertrag geschlossen, der die datenschutzrechtlichen Pflichten und Rechte festlegt?	Ja
Wurden technische und organisatorische Maßnahmen mit dem Auftragsverarbeiter oder gemeinsamen Verantwortlichen vereinbart?	Ja
Bitte beschreiben Sie in kurzen Stichworten die getroffenen technischen und organisatorischen Maßnahmen.	

4. Schritt: Sicherstellung der betroffenen Rechte. Zur Wahrung der betroffenen Rechte ist ein Betroffenenrechteprozess zu etablieren, der für die Beantwortung der Betroffenenanfragen vorgesehen ist. Vor diesem Hintergrund ist Prüfungsgegenstand der etablierte Betroffenenrechteprozess und dessen Effektivität.

Frage	Antwort
Wurde ein Prozess zur Beantwortung der Betroffenenanfragen etabliert?	Ja
Wurden interne Verantwortlichkeiten definiert?	Ja
Wenn die vorherigen Fragen mit „Ja“ beantwortet wurden, beschreiben Sie den Betroffenenrechteprozess und nennen Sie die Position der Verantwortlichkeiten.	
Wurde die 1-Monats-Frist bisher überschritten?	Ja
Wenn ja, warum? (z.B. Fachbereich hat nicht rechtzeitig die Daten zur Verfügung gestellt)	

Glossar

Begriff	Definition
Personenbezogene Daten	„Personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
Auftragsverarbeiter	„Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, Art. 4 Nr. 8 DSGVO
„Gemeinsame Verantwortlichkeit“	Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche, Art. 26 Abs. 1 DSGVO.

7 LITERATURVERZEICHNIS

Anant, Venky/Donchak, Lisa/Kaplan, James/Soller, Henning: The consumer-data opportunity and the privacy imperative, online abrufbar unter: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative, zuletzt besucht am 27.09.2022.

Arnesen, Petter/Hanne, Seter/Foss, Trond/Dahl, Erlend/Lillestøl, Per Johan/Jenssen, Gunnar: Geofencing for smart urban mobility, 2020, online abrufbar unter: https://sintef.brage.unit.no/sintef-xmlui/bitstream/handle/11250/2643877/2020-00100_Geofencing%2bfor%2bsmart%2burban%2bmobility.pdf?sequence=2&isAllowed=y, zuletzt besucht am 28.09.2022.

Bartsch, Alexander/Roth, Heiko: Zivil- und strafrechtliche Möglichkeiten zur Durchsetzung der gesetzlichen Vorgaben zum Datenschutz am Beispiel arbeitsteiliger Verarbeitungsvorgänge im nicht-öffentlichen Bereich, EnWZ 2018, 435 ff.

Bayrisches Landesamt für Datenschutzaufsicht: Datenschutz-Folgenabschätzung, online abrufbar unter: https://www.lda.bayern.de/de/thema_dsfa.html, zuletzt besucht am 22.09.2022.

Berliner Beauftragte für Datenschutz und Informationsfreiheit: Datenschutz – Rechtliche Grundlagen, online abrufbar unter: https://www.datenschutz-berlin.de/datenschutz/rechtliche-grundlagen, zuletzt besucht am 22.09.2022.

Bitkom: IT-Risiko und Chancenmanagement im Unternehmen – Ein Leitfaden für kleine und mittlere Unternehmen, online abrufbar unter: https://www.bitkom.org/sites/default/files/file/import/060601-Bitkom-Leitfaden-IT-Risikomanagement-V10-final.pdf, zuletzt besucht am 27.09.2022.

Bitkom: Risk Assessment & Datenschutz-Folgenabschätzung, online abrufbar unter: https://www.bitkom.org/sites/main/files/file/import/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf, zuletzt besucht am 22.09.2022.

BMW: Fragen und Antworten der BMW-Kundenbetreuung, online abrufbar unter: https://faq.bmw.de/s/article/My-BMW-App-BMW-Points-Bei-BMW-Points-anmelden-BMW-Points-einlösen-gDjIy?language=de, zuletzt besucht am 22.09.2022.

BMW: Rechtliche Hinweise zum Datenschutz, online abrufbar unter: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi7qZa9m7P6AhUBRvEDHebDCpQQFnoECBQQAQ&url=https%3A%2F%2Fwww.bmw.de%2Fcontent%2Fdam%2Fbmw%2FmarketDE%2Fbmw_de%2Fnew-vehicles%2Fpdf%2FBMW_ConnectedDrive_Datenschutz.pdf&usg=AOvVaw0gQd5S-JtVVakmx2ibZs4R, zuletzt besucht am 26.09.2022.

BMW Group: Elektrisch fahren, BMW Points sammeln, kostenfrei laden: BMW präsentiert weltweit erstes Prämienprogramm für Fahrer von Plug-in-Hybrid-Modellen, online abrufbar unter: https://www.press.bmwgroup.com/deutschland/article/detail/T0318751DE/ elek-risch-fahren-bmw-points-sammeln-kostenfrei-laden:-bmw-praesentiert-weltweit-erstes-praemienprogramm-fuer-fahrer-von-plug-in-hybrid-modellen?language=de, zuletzt besucht am 26.09.2022.

Böhm, Wolf-Tassilo/Brams, Isabelle: Aktuelle Entscheidungen der Arbeitsgerichte zum Beschäftigtendatenschutz, NZA-RR 2021, 521, 521.

Brandt, Mathias: DSGVO-Bußgelder knacken 2021 die Milliardengrenze, online abrufbar unter: https://de.statista.com/infografik/26629/strafen-auf-grund-von-verstoessen-gegen-die-datenschutz-grundverordnung/, zuletzt besucht am 23.09.2022.

Bundesministerium der Justiz und Verbraucherschutz: Corporate Digital Responsibility: Digitalisierung verantwortungsvoll gestalten, online abrufbar unter: https://www.bmj.de/SharedDocs/Downloads/DE/News/Artikel/100818_CDR-Initiative.pdf?__blob=publicationFile&v=4, zuletzt besucht am 26.09.2022.

Bundesministerium für Arbeit und Soziales: Corporate Digital Responsibility, online abrufbar unter: https://www.csr-in-deutschland.de/DE/CSR-Allgemein/Corporate-Digital-Responsibility/corporate-digital-responsibility.html, zuletzt besucht am 22.09.2022.

Bundesministerium für Wirtschaft und Klimaschutz: Datenökonomie, online abrufbar unter: https://www.bmwk.de/Redaktion/DE/Schlaglichter-der-Wirtschaftspolitik/2020/09/kapitel-1-7-auf-einen-blick.html, zuletzt besucht am 23.09.2022.

Bundesregierung: Anreiz für weniger CO2-Emissionen, online abrufbar unter: https://www.bundesregierung.de/breg-de/themen/klimaschutz/weniger-co2-emissionen-1790134, zuletzt besucht am 23.09.2022.

Burger, Anton/Buchhart, Anton: Risiko-Controlling, 1. Auflage, Oldenburg 2002.

CMS: GDPR Enforcement Tracker, online abrufbar unter: https://www.enforcementtracker.com, zuletzt besucht am 22.09.2022.

CNIL: Cookies: Facebook Ireland Limited fined 60 million euros, online abrufbar unter: https://www.cnil.fr/en/cookies-facebook-ireland-limited-fined-60-million-euros, zuletzt besucht am 22.09.2022.

Cooper, Tim/Siu, Jade/Wei, Kuangyi: Corporate digital responsibility – Doing well by doing good, online abrufbar unter: https://www.criticaleye.com/ inspiring/insights-servfile.cfm?id=4431, zuletzt besucht am 26.09.2022.

Christensen/Serafeim/Sikochi: Why is Corporate Virtue in the Eye of The Beholder? The Case of ESG Rating, Boston 2020.

Datenschutzbeauftragter Hamburg: Das Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der TOM, online abrufbar unter: https://datenschutzbeauftragter-hamburg.de/2018/08/das-verfahren-zur-regelmaessigen-ueberpruefung-der-wirksamkeit-der-tom/, zuletzt besucht am 27.09.2022.

Datenschutzbehörde (Republik Österreich): Datenschutzbeschwerde (Art. 77 Abs. 1 DSGVO), online abrufbar unter: https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk_0.pdf, zuletzt besucht am 22.09.2022.

Datenschutzkonferenz: Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich, online abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_ google_analytics.pdf, zuletzt besucht am 27.09.2022.

Datenschutzkonferenz: Kurzpapier Nr. 14: Beschäftigtendatenschutz, online abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/ dsk_kpnr_14.pdf, zuletzt besucht am 26.09.2022.

Datenschutzkonferenz: Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, online abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/ dsk_kpnr_5.pdf, zuletzt besucht am 26.09.2022.

Datenschutzkonferenz: Orientierungshilfe der Aufsichtsbehörden für Anbieter*innen von Telemedien ab dem 1. Dezember 2021, online abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien. pdf, zuletzt besucht am 27.09.2022.

Datenschutzkonferenz: Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, online abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_ whistleblowing_hotlines.pdf, zuletzt besucht am 26.09.2022.

Datenschutz.org. Datenschutz während der Corona-Pandemie: Was ist erlaubt, was nicht?, online abrufbar unter: https://www.datenschutz.org/corona/, zuletzt besucht am 26.09.2022.

Datenschutz.org. : Vorratsdatenspeicherung – Stehen alle Menschen unter Generalverdacht?, online abrufbar unter: https://www.datenschutz.org/vorrats-datenspeicherung/, zuletzt besucht am 27.09.2022.

Dehmel, Susanne: Datenschutz als Daueraufgabe für die Wirtschaft: DS-GVO & internationale Datentransfers, online abrufbar unter: https://www.bitkom.org/sites/default/files/ 2021-09/bitkom-charts-pk-datenschutz-15-09-2021.pdf, zuletzt besucht am 23.09.2022.

Dein Geld anlegen: ESG Rating & Agenturen – Übersicht: Welche gibt es?. online abrufbar unter: https://www.dein-geld-anlegen.de/esg-rating-agenturen-uebersicht/, zuletzt besucht am 28.09.2022.

Deiwick, Hartmut: Droht das Aus für Google Analytics in der EU?, ZD 2022, 01125.

Delhaes, Daniel: Mangelnder Datenschutz: Justizministerium lehnt Scheuers Gesetz zum autonomen Fahren ab, online abrufbar unter: https://www.handelsblatt.com/politik/deutschland/plaene-des-verkehrsministers-mangelnder-datenschutz-justizministerin-lehnt-scheuers-gesetz-zum-autonomen-fahren-ab/26830532.html, zuletzt besucht am 23.09.2022.

Deloitte: Datenschutz-Organisation, online abrufbar unter: https://www2.deloitte.com/de/de/pages/risk/articles/datenschutz-organisation.html, zuletzt besucht am 22.09.2022.

Deloitte: Smart Home Consumer Survey 2018 – Ausgewählte Ergebnisse für den deutschen Markt, online abrufbar unter: https://www2.deloitte.com/de/de/pages/ technology-media-and-telecommunications/articles/smart-home-studie-2018.html, zuletzt besucht am 26.09.2022.

Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit: 35,3 Millionen Euro Bußgeld wegen Datenschutzverstößen im Servicecenter von H&M, online abrufbar unter: https://datenschutz-hamburg.de/pressemitteilungen/2020/ 10/2020-10-01-h-m-verfahren, zuletzt besucht 27.09.2022.

Deutsche Bank: Was ist ESG-Investing?, online abrufbar unter: https://deutschewealth.com/de/our-capabilities/what-is-esg-investing.html, zuletzt besucht am 25.09.2022.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit: 47. Tätigkeitsbericht vom 31.12.2018, online abrufbar unter: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2018_47_TB.pdf, zuletzt besucht am 27.09.2022.

Deutsches Institut für Deutsche Revision e.V.: Checkliste zur Prüfung der Datenschutzorganisation, online abrufbar unter: https://www.diir.de/fileadmin/arbeits-kreise/Checkliste_Datenschutzorganisation.pdf, zuletzt besucht am 27.09.2022.

Ditlev-Simonsen, Caroline: A Guide to Sustainable Corporate Responsibility, 1. Auflage, Cham 2022.

Dörr, Saskia: Praxisleitfaden Corporate Digital Responsibility, 1. Auflage, Bonn 2020.

Dr. Ing. h. c. F. Porsche AG: Verantwortung – Geschäfts- und Nachhaltigkeitsbericht der Porsche AG 2021, online abrufbar unter: https://www.volkswagenag.com/presence/ investor-relation/publications/annual-reports/2022/porsche/Geschäfts-%20und%20Nachhaltigkeitsbericht%202021%20Porsche%20AG.pdf, zuletzt besucht am 27.09.2022.

Ehringer, Wolfgang: Instrumente zur Strategieentwicklung: methodische Unterstützung für Praktiker, 1. Auflage, Wiesbaden 2020.

Elgar, Edward: Research handbook of finance and sustainability, Cheltenham 2018, zitiert als: Bearbeiter, in: Research handbook of finance and sustainability.

Elkington, John: Cannibals with forks: The triple bottom line of 21st century business, Oxford 1997.

European Data Protection Board: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 2019, online abrufbar unter: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, zuletzt besucht am 26.09.2022.

Europäischer Datenschutzausschuss: Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, online abrufbar unter: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_de.pdf, zuletzt besucht am 27.09.2022.

Europäische Kommission: Folgen des Klimawandels, online abrufbar unter: https://climate.ec.europa.eu/climate-change/consequences-climate-change_de, zuletzt besucht am 23.09.2022.

Europäische Kommission: Gemeinsame Erklärung der Europäischen Kommission und der Vereinigten Staaten zum Transatlantischen Datenschutzrahmen, online abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/ip_22_2087, zuletzt besucht am 27.09.2022.

Europäische Kommission: Gerechte und nachhaltige Wirtschaft: Kommission legt Unternehmensregeln für Achtung der Menschenrechte und der Umwelt in globalen Wertschöpfungsketten fest, online abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/ip_22_1145, zuletzt besucht am 23.09.2022.

Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Der europäische Grüne Deal, online abrufbar unter: https://ec.europa.eu/info/sites/default/files/european-green-deal-communication_de.pdf, zuletzt besucht am 23.09.2022.

Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Eine neue EU-Strategie (2011-14) für die soziale Verantwortung der Unternehmen (CSR), online abrufbar unter: https://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri=COM:2011:0681:FIN:DE:PDF, zuletzt besucht am 26.09.2022.

Europäische Kommission: The European Commission and the United States reached an agreement in principle for a Trans-Atlantic Data Privacy Framework, online abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100, zuletzt besucht am 22.09.2022.

Europäische Kommission: Trans-Antlantic Data Privacy Framework, online abrufbar unter: https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/Trans-Atlantic%20Data%20Privacy%20Framework.pdf.pdf, zuletzt besucht am 27.09.2022.

Esselmann, Frank/Golle, Dominik/Thiel, Christian/Brink, Alexander: Corporate Digital Responsibility – Unternehmerische Verantwortung als Chance für die deutsche Wirtschaft, online abrufbar unter: https://zentrum-digitalisierung.bayern/wp-content/uploads/ZD.B-Positionspapier_Final_web.pdf, zuletzt besucht am 26.09.2022.

Fehr, Stefanie: Whistleblowing und Datenschutz – ein unlösbares Spannungsfeld?, ZD 2022, 256, 256.

Financial Sector Initiative: Who Cares Wins, online abrufbar unter: https://www.unepfi.org/fileadmin/events/2004/stocks/who_cares_wins_global_compact_2004.pdf, zuletzt besucht am 25.09.2022.

Freiberg, David/Rogers, Jean/Serafeim, George: How ESG Issues Become Financially Material to Corporations and Their Investors, online abrufbar unter: https://deliverypdf.ssrn.com/delivery.php?ID=489024064102117109085070108103098064027075072041043035077074026004118008104122066072123098043034107058119101124071101095091068059012026078015004085122071126097086032085044066095076113085071120118125002083094018121010097067123005011088112076094003118&EXT=pdf&INDEX=TRUE, zuletzt besucht am 27.09.2022.

Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA): Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge, online abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/DSK_20160126_VernetzteKfz.pdf;jsessionid=C1ABCB7E9FE521770B38BA33B9B81753.intranet221?__blob=publicationFile&v=3, zuletzt besucht am 26.09.2022.

Gesellschaft für Datenschutz und Datensicherheit e.V.: Datenschutz und Corona, online abrufbar unter: https://www.gdd.de/datenschutz-und-corona, zuletzt besucht am 26.09.2022.

Gesellschaft für Datenschutz und Datensicherheit e.V.: Voraussetzungen der Datenschutz-Folgenabschätzung, online abrufbar unter: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_10.pdf, zuletzt besucht am 26.09.2022.

GeSI: Kategorisierung der 17 UN-Ziele in die ESG-Dimensionen, Digital with Purpose: Delivering a SMARTer2030, online abrufbar unter: https://gesi.org/platforms/digital-with-a-purpose-delivering-a-smarter2030m, zuletzt besucht am 28.09.2022.

Giese, Guido/Nagy, Zoltán/Lee: Welche ESG-Kriterien waren die wichtigsten? Definition von Ereignis- und Erosionsrisiken, online abrufbar unter: https://www.msci.com/www/blog-posts/welche-esg-kriterien-waren-die/02195301241, zuletzt besucht am 27.09.2022.

Gleißner, Werner/Füser, Karsten: Praxishandbuch Rating und Finanzierung, 3. Auflage, München 2014.

Global Intelligence for the CIO: The rise of corporate digital responsibility, online abrufbar unter: https://www.i-cio.com/management/best-practice/item/the-rise-of-corporate-digital-responsibility, zuletzt besucht am 26.09.2022.

Global Sustainable Investment Alliance: Global Sustainable Investment Review 2020, 2021.

Greiten, Thorsten: Übersicht über die wichtigsten ESG-Ratings – und was sie für die Finanzkommunikation bedeuten, online abrufbar unter: https://www.netfed.de/blog/uebersicht-ueber-die-wichtigsten-esg-rankings-und-was-sie-fuer-die-finanzkommunikation-bedeuten/, zuletzt besucht am 27.09.2022.

GRI Standards: GRI 418: Customer Privacy 2016, online abrufbar unter: https://www.globalreporting.org/standards/media/1033/gri-418-customer-privacy-2016.pdf, zuletzt besucht am 28.09.2022.

Grober, Ulrich: Die Entdeckung der Nachhaltigkeit: Kulturgeschichte eines Begriffs, 3. Edition, München 2010.

Grosvenor/Patel/Lowe/Donati: A Foundation for Better Compliance?, online abrufbar unter: https://www.alvarezandmarsal.com/insights/esg-and-privacy-foundation-better-compliance, zuletzt besucht am 23.09.2022.

Google: Funktionsweise von Google Analytics, online abrufbar unter: https://support.google.com/analytics/answer/12159447?hl=de&ref_topic=12156336&visit_id=637992072377954416-527336403&rd=1, zuletzt besucht am 27.09.2022.

Google Analytics-Hilfe: Funktionsweise von Google Analytics, online abrufbar unter: https://support.google.com/analytics/answer/12159447?authuser=1&hl=de&authuser=1&ref_topic=12156336,12153943,2986333,&visit_id=637915204297548005-595841215&rd=1, zuletzt besucht am 22.09.2022.

Götz, Sören: Als hätte man 360.000 Autos stillgelegt, online abrufbar unter: https://www.zeit.de/mobilitaet/2021-02/co2-steuer-klimaschutz-preiserhoehung-autofahrer-pandemie, zuletzt besucht am 28.09.2022.

Gruenderfreunde: Was ist Nachhaltigkeit?, online abrufbar unter: https://gruenderfreunde.de/was-ist-nachhaltigkeit/, zuletzt besucht am 23.09.2022.

Haake, Klaus/Rusch, Josef/Seiler, Willi/Seliner, Patrick: Strategie-Workshop, 4. Auflage, St. Gallen 2020.

Hamm, Christoph: Beck'sches Rechtsanwalts-Handbuch, 12. Auflage, München 2022, zitiert als: Bearbeiter, in: Beck'sches Rechtsanwalts-Handbuch.

Hanschke, Inge: Informationssicherheit und Datenschutz, 1. Auflage, Wiesbaden 2019.

Hayat, Usman: Environmental, Social, and Governance Issues In Investing, online abrufbar unter: https://www.cfainstitute.org/en/advocacy/policy-positions/environmental-social-and-

governance-issues-in-investing-a-guide-for-investment-professionals, zuletzt besucht am 25.09.2022.

Heawood: Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal, 2018, online abrufbar unter: https://content.iospress.com/download/ in-formation-polity/ip180009?id=information-polity%2Fip180009, zuletzt besucht am 26.09.2022.

Hubard, Douglas W./Seiersen, Richard: How to Measure Anything in Cyber Security Risk, 1. Auflage, Weinheim 2016.

Intersoft Consulting: DSGVO Privacy by Design, online abrufbar unter: https://dsgvo-gesetz.de/themen/privacy-by-design/m, zuletzt besucht am 27.09.2022.

Jena, Anupam: US drug prices higher than in the rest of the world, here's why, online abrufbar unter: https://thehill.com/opinion/healthcare/369727-us-drug-prices-higher-than-in-the-rest-of-the-world-heres-why/, zuletzt besucht am 27.09.2022.

Jung, Markus: Scalable Capital soll wegen Datendiebstahl zahlen, online abrufbar unter: https://www.faz.net/aktuell/wirtschaft/scalable-capital-soll-wegen-datendiebstahl-nach-dsgvo-zahlen-17695455.html, zuletzt besucht am 27.09.2022.

Kayser, Thomas: 1,5 Mio. Euro Bußgeld wegen massiven Lecks bei Gesundheitsdaten, online abrufbar unter: https://www.activemind.de/magazin/bussgeld-gesundheitsdaten/, zuletzt besucht am 22.09.2022.

Keller, Axel: Datenübermittlung in die USA? – Jetzt wird bundesweit geprüft, online abrufbar unter: https://www.ecovis.com/datenschutzberater/datenuebermittlung-in-die-usa-jetzt-wird-bundesweit-geprueft/, zuletzt besucht am 27.09.2022.

Klipper, Sebastian: Information Security Risk Management, 2. Auflage, Wiesbaden 2015.

Knupp, Adriana: CO2-Steuer in Deutschland – Kosten, Berechnung und Co. – alles was Sie wissen müssen, online abrufbar unter: https://www.wiwo.de/finanzen/steuern-recht/co2-steuer-in-deutschland-2022-kosten-berechnung-und-co-alles-was-sie-zur-kohlenstoffsteuer-wissen-muessen/25533826.html, zuletzt besucht am 23.09.2022.

Kretzmann, Tobias Malte: Analyse und Implementierung eines Datenschutzmanagementsystems (DSMS) gemäß Datenschutz-Grundverordnung (DSGVO) in ein bestehendes Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 am Beispiel eines mittelständischen Unternehmens, online abrufbar unter: https://reposit.haw-hamburg.de/bitstream/20.500.12738/8963/1/Kretzmann_geschwaerzt.pdf, zuletzt besucht am 27.09.2022.

Kühl, Eike: Facebook – Kongress 2:0, online abrufbar unter: https://www.zeit.de/digital/internet/2018-04/mark-zuckerberg-facebook-us-kongress-datenmissbrauch-anhoerung?page=11, zuletzt besucht am 27.09.2022.

Litz, Jürgen: CRM und Datenschutz – ziemlich beste Freunde!, online abrufbar unter: https://www.cobra.de/crm-und-datenschutz/dsgvo-interviews-beitraege/crm-und-datenschutz-ziemlich-beste-freunde, zuletzt besucht am 27.09.2022.

LDA Bayern: Datenschutz-Folgenabschätzung, online abrufbar unter: https://www.datenschutz-bayern.de/dsfa/, zuletzt besucht am 26.09.2022.

Leibold, Kevin: Schadensersatzansprüche sowie Inhalt und Streitwerte des Auskunftsanspruchs nach der DS-GVO, ZD 2022, 18, 38.

Leuering, Dieter /Rubner, Daniel: Lieferkettensorgfaltspflichtengesetz, NJW-Spezial, 399, 400.

Leupold, Andreas/Wiebe, Andreas/Glossner, Silke: IT-Recht – Recht, Wirtschaft und Technik der digitalen Transformation, 4. Auflage, München 2021, zitiert als: Bearbeiter, in: IT-Recht.

Liu, Jess: ESG Investing Comes of Age, online abrufbar unter: https://www.morningstar.com/features/esg-investing-history, zuletzt besucht am: 25.09.2022.

Lombriser, Roman/Abplanapl, Peter A.: Strategisches Management, 7. Auflage, Zürich 2018.

Loomans, Dirk/Matz, Manuela/Wiedemann, Michael: Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems, 1. Auflage, Wiesbaden 2014.

López, Elena Esnaola: Nachhaltigkeit und Datenschutz: Neues von der CDR-Initiative, online abrufbar unter: https://www.basecamp.digital/nachhaltigkeit-und-datenschutz-neues-von-der-cdr-initiative/, zuletzt besucht am 23.09.2022.

Matos, Pedro: ESG and Responsible Institutional Investing Around the World – A Critical Review, Virginia 2020.

Matzler, Kurt/Müller-Seeger, Julia/Hautz, Julia/Mooradian, Todd: Strategisches Management – Konzepte und Methoden, 3. Auflage, Wien 2021.

Mauss Datenschutz GmbH: Das Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der TOM, online abrufbar unter: https://datenschutzbeauftragter-hamburg.de/2018/08/das-verfahren-zur-regelmaessigen-ueberpruefung-der-wirksamkeit-der-tom/, zuletzt besucht am 22.09.2022.

McKinsey & Company: The consumer-data opportunity and the privacy imperative, online abrufbar unter: https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative, zuletzt besucht am 22.09.2022

MSCI: MSCI ESG Ratings Methodology, online abrufbar unter: https://www.msci.com/documents/1296102/21901542/ESG-Ratings-Methodology-Exec-Summary.pdf, zuletzt besucht am 27.09.2022.

MSCI: The Global Industry Classification Standard, online abrufbar unter: https://www.msci.com/our-solutions/indexes/gics, zuletzt besucht am 27.09.2022.

MSCI: What You Need to Know About MSCI ESG, online abrufbar unter: https://www.setsustainability.com/download/svpc3g1kuxnljdy, zuletzt besucht am 27.09.2022.

Morgan Stanley Capital International: MSCI ESG Government Ratings, online abrufbar unter: https://www.msci.com/our-solutions/esg-investing/esg-ratings, zuletzt besucht am 23.09.2022.

Morgan Stanley Capital International: The Global Industrie Classification Standard (GICS), online abrufbar unter: https://www.msci.com/our-solutions/indexes/gics, zuletzt besucht am 22.09.2022.

Nait-Sidi-Moh, Ahmed/Bakhouya, Mohamed/Gaber, Jaafar/Wack, Maxime: Geopositioning and Mobility, 1. Auflage, London 2013.

National Acadamies: Geofencing for Smart Urban Mobility: Effects From a Pilot With Retrofit Equipment, online abrufbar unter: https://trid.trb.org/view/1769375, zuletzt besucht am 26.09.2022.

Neuerer, Dietmar: Stefan Brink: „Unternehmen sind mit einer massiven Bußgeldgefahr konfrontiert“, online abrufbar unter: https://www.handelsblatt.com/politik/ deutschland/datenschuetzer-im-interview-stefan-brink-unternehmen-sind-mit-einer-massiven-bussgeldgefahr-konfrontiert/26851202.html, zuletzt besucht am 27.09.2022.

New York Times: Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, online abrufbar unter: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html, zuletzt besucht am 26.09.2022.

NOYB: NOYB enforces your right to privacy everyday, online abrufbar unter: https://noyb.eu/en, zuletzt besucht am 23.09.2022.

Ottoschmidt: Datenschutzrechtliche Empfehlungen zum automatisierten und vernetzten Fahren, online abrufbar unter: https://www.otto-schmidt.de/news/wirtschaftsrecht/bfdi-zum-datenschutz-beim-automatisierten-und-vernetzten-fahren-2017-06-09.html, zuletzt besucht am 26.09.2022.

Patrizio, Andy: IDC: Expect 175 zettabytes of data worldwide by 2025, online abrufbar unter: https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html, zuletzt besucht am 23.09.2022.

Plankemann, Michael: Datenschutz-Managementsystem im Unternehmen, online abrufbar unter: https://www.activemind.de/magazin/datenschutz-management-im-unternehmen/, zuletzt besucht am 23.09.2022.

PWC: Unterstützt Ihr Datenschutzprogramm Ihre ESG-Bemühungen?, online abrufbar unter: https://www.pwc.ch/de/insights/regulierung/datenschutz-and-esg.html, zuletzt besucht am 26.09.2022.

Rat für nachhaltige Entwicklung: Nachhaltige Entwicklung, online abrufbar unter: https://www.nachhaltigkeitsrat.de/nachhaltige-entwicklung/, zuletzt besucht am 23.09.2022.

Redclover Advisors: Data Privacy & ESG, online abrufbar unter: https://redcloveradvisors.com/2021/05/21/data-privacy-esg-2/, zuletzt besucht am 26.09.2022.

Regierungskommission: Deutscher Corporate Governance Kodex, online abrufbar unter: https://www.dcgk.de//files/dcgk/usercontent/de/download/kodex/220627_Deutscher_Corporate_Governance_Kodex_2022.pdf, zuletzt besucht am 25.09.2022.

RMA Risk Management & Rating Association e.V.: Risikoquantifizierung Grundlagen – Werkzeuge – Praxisbeispiele, Band 6, Berlin 2022.

Reusch, Philipp: Mobile Updates – Updatability, Update-Pflicht und produkthaftungsrechtlicher Rahmen, BB 2019, 904, 905 f.

Ronellenfitsch, Michael: Siebenundvierzigster Tätigkeitsbericht zum Datenschutz und Erster Bericht zur Informationsfreiheit des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, online abrufbar unter: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2018_47_TB.pdf, zuletzt besucht am 22.09.2022.

Sahin, Özge/Bax, Karoline/Czado, Claudia/Paterlini, Sandra: Environmental, Social, Governance scores and the missing pillar – Why does missing information matter?, online abrufbar unter: https://arxiv.org/pdf/2106.15466.pdf, zuletzt besucht am 27.09.2022.

Schawel, Christian/Billing, Fabian: Top 100 Management Tools, 6. Auflage, Wiesbaden 2018.

Schier, Susanne: Nach Datenleck: Scalable Capital soll Schadenersatz zahlen, online abrufbar unter: https://www.handelsblatt.com/finanzen/banken-versicherungen/banken/urteil-nach-datenleck-scalable-capital-soll-schadensersatz-zahlen/27916910.html?ticket=ST-10991260-YfxxHksOLyrRZkcEKRsu-cas01.example.org, zuletzt besucht am 27.09.2022.

Schmidbauer/Willmroth: Öko-Fonds schmeißen Volkswagen raus, online abrufbar unter: https://www.sueddeutsche.de/geld/aktien-oeko-fonds-schmeissen-volkswagen-raus-1.2670144, zuletzt besucht am 25.09.2022.

Schneider, Andreas/Schmidpeter, René: Corporate Social Responsibility – Verantwortungsvolle Unternehmensführung in Theorie und Praxis, 2. Auflage, Köln 2015.

Schröder, Georg F.: Datenschutzrecht für die Praxis, 4. Auflage, München 2021.

Schuh/Zeller/Stich: Digitalisierungs- und Informationsmanagement, 1. Auflage, Heidelberg 2022.

Schwarzer, Christoph M.: Die Sogwirkung der Subventionen, online abrufbar unter: https://www.zeit.de/mobilitaet/2021-10/plug-in-hybridautos-subventionen-kritik-elektromobilitaet-verkehrswende, zuletzt besucht am 26.09.2022.

Schwemberger, Antje: SDG Talk Nachhaltige Werte im Unternehmen? Wozu? – Strategiearbeit als Erfolsfaktor, online abrufbar unter: https://www.wko.at/service/t/umwelt-energie/sdg-talk-experten-thema-nachhaltigkeitsziele.html, zuletzt besucht am 18.10.2022.

Shah, Raj: ESG and Data Protection, online abrufbar unter: https://collyerbristow.com/shorter-reads/esg-and-data-protection/, zuletzt besucht am 23.09.2022.

Sherwood, Matthew W. /Pollard, Julia: Responsible Investing – An Introduction to Environmental, Social and Governance Investment, Abingdon 2018.

Smart-Data-Begleitforschung: Corporate Digital Responsibility, online abrufbar unter: https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2018_02_smartdata_corporate_digital_responsibility.pdf%3F__blob%3DpublicationFile%26v%3D8, zuletzt besucht am 26.09.2022.

Sorber, Dominik: Wann kommt der Schutz für Whistleblower?, online abrufbar unter: https://www.lto.de/recht/hintergruende/h/bag-2azr23521-auskunft-dsgvo-kopie-anspruch-arbeitnehmer-arbeitgeber-whistleblower-hinweisgeber/, zuletzt besucht am 22.09.2022.

Sourcing International: Die Nutzung von Google Analytics ist nicht DSGVO konform – Neue Grundsatzentscheidung der österreichischen Datenschutzbehörde, online abrufbar unter: https://sourcing-international.org/news/article/die-nutzung-von-google-analytics-ist-nicht-dsgvo-konform-neue-grundsatzentscheidung-der-oesterreich/, zuletzt besucht am 22.09.2022.

Specht, Louisa/Mantz, Reto: Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage, München 2019, zitiert als: Bearbeiter, in: Handbuch Europäisches und deutsches Datenschutzrecht.

Specht-Riemenschneider: Herstellerhaftung für nicht-datenschutzkonform nutzbare Produkte – Und er haftet doch!, MMR 2020, 73, 75.

Stöbener de Mora, Patricia/Noll, Paul: Grenzenlose Sorgfalt? – Das Lieferkettensorgfaltspflichtengesetz, NZG, 1237, 1244.

Stöger, Roman: Strategieentwicklung für die Praxis, 3. Auflage, Stuttgart 2017.

Streda, Adolf: Der mündige (gläserne) Nutzer?, online abrufbar unter: https://www.funkschau.de/sicherheit-datenschutz/der-muendige-glaeserne-nutzer.182964.html, zuletzt besucht am 23.09.2022.

Townsend, Blaine: From SRI to ESG: The Origins of Socially Responsible and Sustainable Investment, San Francisco 2020.

U.a. Hansen, Lillian/Peter, Arnesen/Sven-Thomas, Graupner: Current state of the art and use case description on geofencing for traffic management, online abrufbar unter: https://sintef.brage.unit.no/sintef-xmlui/bitstream/handle/11250/2826636/GeoSence.%2b Current%2bstate%2bof%2bthe%2bart%2band%2buse%2bcase%2bdescription% 2bon%2bgeofencing%2bfor%2btraffic%2bmanagement.pdf?sequence=1&isAllowed=y, zuletzt besucht am 26.09.2022.

U.a. Herden, Christina J./Alliu, Ervin/Cormier, Thibaut: Corporate Digital Responsibility, 2021, online abrufbar unter: https://link.springer.com/content/pdf/10.1007/s00550-020-00509-x.pdf, zuletzt besucht am 26.09.2022.

Umweltbundesamt: Soziale Aspekte des Umweltschutzes/Ökologische Gerechtigkeit, online abrufbar unter: https://www.umweltbundesamt.de/themen/nachhaltigkeit-strategien-internationales/soziale-aspekte-des-umweltschutzesoekologische, zuletzt besucht am 26.09.2022.

Unabhängiges Datenschutzzentrum Saarland: 27. Tätigkeitsbericht, online abrufbar unter: https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/tberichte/tb27_1718.pdf, zuletzt besucht am 26.09.2022.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Tätigkeitsbericht 2019, online abrufbar unter: https://www.datenschutzzentrum.de/tb/tb37/uld-37-taetigkeitsbericht-2019.pdf, zuletzt besucht am 26.09.2022.

United Nations: Do you know all 17 SDGs?, online abrufbar unter: https://sdgs.un.org/goals, zuletzt besucht am 17.10.2022.

United Nations: Our Common Future: Report of the World Commission on Environment and Development, Oslo 1987.

United Nations Environment Programme Finance Initiative : A legal framework for the integration of environmental, social and governance issues into institutional investment, online abrufbar unter: https://www.unepfi.org/fileadmin/documents/freshfields_legal_resp_20051123.pdf, zuletzt besucht am 25.09.2022.

Vanini, Ute: Risikomanagement Grundlagen – Instrumente – Unternehmenspraxis, 2. Auflage, Stuttgart 2021.

Verband der Automobilindustrie (VDA): Drei Prinzipien für den Datenschutz beim autonomen und vernetzten Fahren, online abrufbar unter: https://www.vda.de/de/themen/digitalisierung/daten/datenschutz, zuletzt besucht am 26.09.2022.

Voigt/von dem Bussche: EU-Datenschutzgrundverordnung (DSGVO) – Praktikerhandbuch, 1. Auflage, Berlin 2018.

Volkswagen AG: Geschäfts- und Nachhaltigkeitsbericht 2021 von Dr. Ing. h. c. F. Porsche AG, online abrufbar unter: https://www.volkswagenag.com/presence/investorrelation/ publications/annual-reports/2022/porsche/Geschäfts-%20und%20Nachhaltigkeitsbericht% 202021%20Porsche%20AG.pdf, zuletzt besucht am 22.09.2022.

Von dem Bussche, Alex Frhr./Voigt, Paul: Konzerndatenschutz Rechtshandbuch, 2. Auflage, München 2019, zitiert als: Bearbeiter, in: Konzerndatenschutz Rechtshandbuch.

Von Wirth, Sophie/Liedke, Janine: Was die CO2-Steuer für Verbraucher bedeutet, online abrufbar unter: https://www.handelsblatt.com/finanzen/steuern-recht/steuern/co2-preis-was-die-co2-steuer-fuer-verbraucher-bedeutet/26228322.html, zuletzt besucht am 23.09.2022.

Wagner-Havlicek, Carina/ Wimmer, Harald: Werbe- und Kommunikationsforschung, 1. Auflage, Baden-Baden 2020, zitiert als: Bearbeiter, in: Werbe- und Kommunikationsforschung.

Weber, Jürgen/Georg, Johannes/Janke, Robert/Mack, Simone: Nachhaltigkeit und Controlling, 1. Auflage, Weinheim 2012.

Weber, Peter/Gabriel, Roland/Lux, Thomas/Menke, Katharina: Basiswissen Wirtschaftsinformatik, 4. Auflage, Wiesbaden 2022.

Weihrich, Heinz: The TOWS Matrix – A Tool for Situational Analysis, online abrufbar unter: https://reader.elsevier.com/reader/sd/pii/0024630182901200?token=E7BD21B49D6DA2B8361D2F9A525D5A99C4CDE35C5F335306A56DBF3479DD70CD9B165569990F6EF4F4F585F12BB306FE&originRegion=eu-west-1&originCreation=20220928115244, zuletzt besucht am 28.09.2022.

WEKA : Lieferkettengesetz: praktische Umsetzung in Unternehmen, online abrufbar unter: https://www.weka.de/umweltschutz/was-das-lieferkettengesetz-fuer-ihr-unternehmen-bedeutet/, zuletzt besucht am 26.09.2022.

Welthungerhilfe: Naturkatastrophen und der Klimawandel, online abrufbar unter: https://www.welthungerhilfe.de/informieren/themen/klimawandel/naturkatastrophen, zuletzt besucht am 26.09.2022.

Wicharz, Ralf: Strategie: Ausrichtung von Unternehmen auf die Erfolgslogik ihrer Industrie, 3. Auflage, Wiesbaden 2018.

Wolff, Amadeus Heinrich/Brink, Stefan: BeckOK Datenschutzrecht, 41. Edition, München 2022, zitiert als: Bearbeiter; in: Beck`sche OK.

ZEIT ONLINE: WhatsApp muss Strafe von 225 Millionen Euro zahlen, online abrufbar unter: https://www.zeit.de/digital/2021-09/whatsapp-irland-bussgeld-rekordstrafe-datenschutz-millionen-facebook?utm_referrer=https%3A%2F%2Fwww.google.com%2F, zuletzt besucht am 22.09.2022.

Rechtsprechungsverzeichnis

EuGH, Urteil vom 16.7.2022 – C-311/18, NJW 2020, 2613, 2613.

EuGH (Große Kammer), Urteil vom 21.12.2016 – C-203/15, C-698/15, EuZW 2017, 153, 160.

EuGH, Urteil vom 13.5.2014 – C-131/12, ZD 2014, 356, 361.

BVerfG, Urteil des Ersten Senats vom 15.12.1983 – 1 BvR 209/83, NJW 1307, 1307 ff.

BAG, Urteil vom 16.12.2021 – Az. 2 AZR 235/21, Legal Tribune Online.

BAG, Urteil vom 27.4.2021 – Az. 2 AZR 342/20, ZD 2021, 589, 591.

OLG Frankfurt a.M., Urteil vom 14.4.2022 – 3 U 21/20, BKR, 534, 539, Rn. 51. LG Lüneburg, Urteil vom 14.7.2020 – 9 O 145/19, BKR, 306, 308, Rn. 51.

LAG Baden-Württemberg, Urteil vom 20.12.2018 – 17 Sa 11/18 (ArbG Stuttgart); nicht rechtskräftig, ZD 2019, 276, mAnm Wybitul.

VG Wiesbaden, Urteil vom 17.1.2022 – 6 K 1164/21. WI, ZD 2022, 406, 409.

VG Lüneburg, Teilurteil vom 19.3.2019 – 4 A 12/19ZD 2019, 331 Rn. 62.

ArbG Münster, Urteil vom 25.3.2021 – 3 Ca 391/20, ZD 2021, 534, 534.

ArbG Bonn, Urteil vom 16.7.2020 – 3 Ca 2026/19, ZD 2021, 111, 111 ff.

Internationale Urteile

Österreichische Datenschutzbehörde, Bescheid vom 22.12.2021, D155.027 2021-0.586.257, S. 18, Spruchpunkt C.9.

8 AUTORENINFORMATION

Valona Avdimetaj LL.M. ist Absolventin des Masterstudiengangs Legal Management an der Hochschule Konstanz. Sie ist bei der KPMG AG als Consultant mit dem Schwerpunkt Datenschutz tätig.

Prof. Dr. Dirk Loomans ist Partner im Bereich Security Consulting von KPMG und seit mehr als 20 Jahren in der Informationssicherheit tätig und hat dabei nationale und internationale Kunden verschiedenster Größen beraten. Seine Beratungsschwerpunkte sind ISMS, Datenschutz, Industriekontrollsysteme, quantitative und qualitative Risikoanalysen. Zudem ist er seit 2011 Professor für Wirtschaftsinformatik an der Hochschule Mainz.

Dr. Thomas Zerres ist Professor für Zivil- und Wirtschaftsrecht an der Hochschule Konstanz. Seine Lehr- und Forschungsschwerpunkte sind neben dem Zivilrecht vor allem das Marketingrecht sowie das Europäische Privatrecht.