Paul Voigt
Axel von dem Bussche

EU-Datenschutz-Grundverordnung (DSGVO)

Praktikerhandbuch

2. Auflage

Springer

EU-Datenschutz-Grundverordnung (DSGVO)

Paul Voigt • Axel von dem Bussche

EU-Datenschutz-Grundverordnung (DSGVO)

Praktikerhandbuch

2. Auflage

Springer

Paul Voigt
Taylor Wessing
Berlin, Deutschland

Axel von dem Bussche
Taylor Wessing
Hamburg, Deutschland

ISBN 978-3-662-68819-9 ISBN 978-3-662-68820-5 (eBook)
https://doi.org/10.1007/978-3-662-68820-5

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über https://portal.dnb.de abrufbar.

Planung/Lektorat: Brigitte Reschke
Springer ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Vorwort

Sechs Jahre ist es her, seitdem die Erstauflage dieses Handbuchs erschienen ist. Seitdem hat sich viel getan. Waren datenschutzrechtliche EuGH-Urteile in Vor-DSGVO-Zeiten noch ein „Event", auf das man sich monatelang „freuen" und vorbereiten konnte, ist es inzwischen eine Herausforderung, der Masse an Datenschutzurteilen und Behördenentscheidungen Herr zu werden. Hinzu kommt eine deutlich zunehmende Digitalregulierung auf europäischer Ebene, die auch auf datenschutzrechtliche und IT-sicherheitsrechtliche Vorgaben Einfluss nimmt – NIS2, DORA, DSA, DMA, AI Act, CRA; die Liste ließe sich beliebig fortsetzen.

Kurzum, eine Neuauflage war angezeigt. Wie bereits in der Vorauflage gehen wir nicht nur auf die DSGVO, sondern auch auf das begleitende deutsche Recht ein, und wie bei der Vorauflage gibt es ein englischsprachiges „Schwesterbuch", das parallel erscheint und die Befassung mit dem Datenschutz im internationalen Kontext erleichtern soll.

Auch in dieser Auflage ist dem Handbuch eine „Checkliste" der wichtigsten Datenschutzpflichten vorangestellt, die maßgebliche Problemfelder in Kurzform darlegt und Verweise auf die entsprechenden Teile dieses Buches enthält.

Für die umfassende Unterstützung bei beiden Projekten möchten wir uns bei Frau Dr. Brigitte Reschke und Frau Julia Bieler vom Verlag Springer Nature, sowie unseren wissenschaftlichen Mitarbeitern Jin Fuhrken, Hannes Bastians, Albert Gutman und Alea Mostler bedanken.

Stets dankbar sind wir auch für Hinweise, Anregungen und Kritik zu diesem Buch, die Sie gerne per Email an p.voigt@taylorwessing.com oder a.bussche@taylorwessing.com richten können.

Berlin, Deutschland — Paul Voigt
Hamburg, Deutschland — Axel Freiherr von dem Bussche
Mai 2024

Inhaltsverzeichnis

Einleitung und „Checkliste“

1

Die rechtlichen Anforderungen an Datenverarbeitungen unterliegen stetem Wandel und für Unternehmen bleibt es eine Herausforderung festzustellen, ob ihre Datenverarbeitungstätigkeiten gesetzeskonform sind. Dies gilt vor allem im internationalen Kontext. Daten können naturgemäß ohne weiteres Landesgrenzen überwinden und spielen in der globalen digitalen Wirtschaft eine zentrale Rolle. Sie haben sich zu einem wertvollen Wirtschaftsgut entwickelt und werden bereits als „Währung der Zukunft“ bezeichnet.[1] Die Verarbeitung personenbezogener Daten findet im Rahmen zahlloser wirtschaftlicher und sozialer Tätigkeiten statt, wobei Fortschritte in der Informationstechnik die Verarbeitung und den Austausch dieser Daten immer mehr erleichtern.[2] In diesem Zusammenhang hat der europäische Gesetzgeber die DSGVO verabschiedet, um eine weitergehende Harmonisierung der Datenschutzregeln innerhalb der EU-Mitgliedstaaten zu erreichen und das Datenschutzniveau zugunsten der von der Verarbeitung betroffenen Personen zu erhöhen. Aufgrund ihres äußerst weiten, transnationalen Anwendungsbereichs findet sie auch auf zahllose Unternehmen außerhalb der EU Anwendung.

1.1 Gesetzgeberischer Hintergrund und bisherige Rechtslage

1.1.1 Die EG-Datenschutzrichtlinie

Vor mehr als 20 Jahren erkannte die damals noch Europäische Gemeinschaft (jetzt: Europäische Union) die Notwendigkeit zur Angleichung der Datenschutzstandards in ihren Mitgliedstaaten, um grenzüberschreitende Datenübertragungen innerhalb

[1] Reiners, ZD 2015, 51, 55.

[2] ErwGr. 4 EG-Datenschutzrichtlinie.

P. Voigt, A. von dem Bussche, *EU-Datenschutz-Grundverordnung (DSGVO)*,
https://doi.org/10.1007/978-3-662-68820-5_1

der EG (jetzt: EU) zu erleichtern. Zur damaligen Zeit wichen die nationalen Bestimmungen zum Datenschutz stark voneinander ab und konnten keine Rechtssicherheit in Bezug auf grenzüberschreitende Verarbeitungsvorgänge bieten – weder für betroffene Personen noch für Verantwortliche oder Auftragsverarbeiter.[3]

1995 verabschiedete die Europäische Gemeinschaft deshalb die *Richtlinie 95/46/EG* des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (kurz: die *EG-Datenschutzrichtlinie*). Zielstellung war es, den Schutz für die Grundrechte und -freiheiten betroffener Personen im Hinblick auf Datenverarbeitungsvorgänge europaweit zu harmonisieren und den freien Datenverkehr zwischen den EU-Mitgliedstaaten zu gewährleisten.[4]

Richtlinien der Europäischen Union sind in den Mitgliedstaaten nicht direkt anwendbar, sondern bedürfen zunächst einer Umsetzung in das nationale Recht. Dafür muss jeder EU-Mitgliedstaat jeweils einen nationalen Umsetzungsrechtsakt erlassen. Aus diesem Grund verfehlte die EG-Datenschutzrichtlinie schließlich ihr Ziel der Angleichung des Datenschutzniveaus innerhalb der EU: auf Grundlage der nationalen Umsetzung bildeten sich zwischen den EU-Mitgliedstaaten unterschiedliche Datenschutz-Regime heraus, die mit den Jahren unterschiedliche Datenschutzniveaus innerhalb der Union zur Folge hatten. Datenverarbeitungstätigkeiten, die in einem EU-Mitgliedstaat rechtskonform waren, konnten in einem anderen Mitgliedstaat im Hinblick auf die spezifische nationale Interpretation der Datenverarbeitung rechtswidrig sein.

1.1.2 Die Datenschutz-Grundverordnung

Im Jahr 2016 verabschiedete der europäische Gesetzgeber die DSGVO, welche die EG-Datenschutzrichtlinie von 1995 ab Mai 2018 ersetzte. Sie ist das Ergebnis eines schwierigen und langen Verhandlungsprozesses, der aufgrund zahlloser Änderungsvorschläge zum Gesetzestext vier Jahre bis zur Verabschiedung der endgültigen Verordnung in Anspruch nahm.

Die aufgezeigte vormalige Fragmentierung des Datenschutzes innerhalb der EU-Mitgliedstaaten und die daraus resultierenden Rechtsunsicherheiten wurden als Hemmnis für die unionsweite Ausübung von Wirtschaftstätigkeiten angesehen und führten zu Wettbewerbsverzerrungen.[5] Im Gegensatz zur EG-Datenschutzrichtlinie ist die DSGVO *direkt anwendbar* – Umsetzungsrechtsakte seitens der EU-Mitgliedstaaten sind nicht mehr erforderlich. Durch die so erzeugte Angleichung der Datenschutzvorschriften sollte die DSGVO zu mehr Rechtssicherheit innerhalb der EU führen und Hindernisse für den grenzüberschreitenden Austausch personenbezogener Daten beseitigen.

---

[3] Polenz, in: Kilian/Heussen, Computerrechts-Handbuch, Teil 13. 131. Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes (2020), Rn. 3.

[4] ErwGr. 3 DSGVO.

[5] ErwGr. 9 DSGVO.

Die EU wollte mit der DSGVO das Vertrauen der Bürger zurückgewinnen. Mit Schaffung eines einheitlichen Rechtsrahmens sollte ein verantwortungsbewusster Umgang mit ihren personenbezogenen Daten sichergestellt werden. Auf dieser Grundlage wollte der europäische Gesetzgeber eine Förderung der digitalen Wirtschaft im europäischen Binnenmarkt erreichen.[6] Unternehmen treffen nach der DSGVO neue Datenschutzpflichten, gleichzeitig werden bereits bestehende datenschutzrechtliche Verpflichtungen verschärft. Der europäische Gesetzgeber hatte für die DSGVO unter Berücksichtigung der Herausforderungen der globalen Wirtschaft, neuer Technologien sowie neuer Geschäftsmodelle einen äußerst weiten Anwendungsbereich vorgesehen. Schließlich wurden nicht nur die datenschutzrechtlichen Pflichten, sondern auch der Bußgeldrahmen signifikant erhöht. Folglich müssen Unternehmen seitdem ihre datenschutzrelevanten Verarbeitungsprozesse einer sorgfältigen Prüfung unterziehen und gegebenenfalls Anpassungen vornehmen, um sie in Einklang mit den Vorgaben der DSGVO zu bringen.

1.1.3 Das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU

Die DSGVO ist als Verordnung in allen ihren Teilen verbindlich und gilt ohne mitgliedstaatlichen Umsetzungsakt unmittelbar.[7] Damit verbleibt den nationalen Gesetzgebern im Anwendungsbereich der DSGVO grundsätzlich keine Regelungsmöglichkeit. Allerdings lässt die DSGVO über *zahlreiche Öffnungsklauseln* den EU-Mitgliedstaaten Raum zur Schaffung ergänzender nationaler Regelungen. Dadurch bestehen weiterhin nationale Besonderheiten im Datenschutzrecht, die hinsichtlich der Praxis jedoch weniger zu einer Fragmentierung des Rechts führen, als zunächst befürchtet.

Als erster EU-Mitgliedstaat hat Deutschland von diesem Gestaltungsspielraum Gebrauch gemacht und bereits im November 2016 – wenige Monate nach Verabschiedung der DSGVO – den ersten Entwurf für ein deutsches Gesetz zur Umsetzung der Verordnung vorgelegt. Das Gesetz dient nicht nur der Ausfüllung des gesetzgeberischen Spielraums gemäß der Öffnungsklauseln der DSGVO, sondern zugleich der Umsetzung der Richtlinie (EU) 2016/680 zum Datenschutz in Strafsachen.[8] Dabei nutzte der deutsche Gesetzgeber jede sich bietende Öffnungsklausel der DSGVO, um möglichst viele Besonderheiten des vorhergehenden deutschen Datenschutzrechts „zu retten“. Dieser als wirtschaftsfreundlich gedachte Regelungs-

[6] ErwGr. 7, 9 DSGVO.

[7] Ruffert, in: Calliess/Ruffert, EUV AEUV, Art. 288 AEUV (2022) Rn. 19 f.; ständige Rspr. bspw. EuGH, Urteil vom 14. Dezember 1971, Politi/Finanzministerium Italien, C-43/71, Rn. 9; EuGH, Urteil vom 17. Mai 1972, Orsolina Leonesio/Ministero dell‘agricoltura e foreste, C-93/71, Rn. 5 f.

[8] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

ansatz bewirkte das Gegenteil, denn für die zunehmend international agierenden Unternehmen führen nationale Sonderwege stets zu Mehraufwand.

Das *Datenschutz-Anpassungs- und -Umsetzungsgesetz EU* ersetzt das alte BDSG und trat im Gleichlauf mit der DSGVO am 25. Mai 2018 in Kraft.[9] Infolge kritischer Stimmen zum Entwurf wurden entsprechende Änderungsvorschläge im Laufe des Gesetzgebungsverfahrens eingearbeitet.[10] Das BDSG wurde schließlich am 27. April 2017 vom Bundestag beschlossen und der Bundesrat stimmte dem Gesetz am 12. Mai 2017 zu. Inwieweit die Regelungen des neuen BDSG mit dem Europarecht, insbesondere der DSGVO, vereinbar sind, ist auch heute noch nicht abschließend geklärt.[11] Zu einem Vertragsverletzungsverfahren, das die Kommission nach Verabschiedung des BDSG angedroht hatte, ist es seit dessen Inkrafttreten allerdings noch nicht gekommen.[12]

1.2 Checkliste – Die wichtigsten datenschutzrechtlichen Pflichten

Für einen kursorischen Überblick über die datenschutzrechtlichen Pflichten nach der DSGVO fasst die nachfolgende „Checkliste“ die *wichtigsten Pflichten* für datenverarbeitende Unternehmen zusammen. Zudem enthält die Liste Verweise auf die entsprechenden Kapitel und Abschnitte dieses Handbuchs.

1.2.1 Datenschutzorganisation

Unternehmen müssen erhebliche Anstrengungen unternehmen, um ihre interne Datenschutzorganisation in Einklang mit den Anforderungen der DSGVO zu bringen. Die DSGVO sieht diverse organisatorische Verpflichtungen vor, welche von Unternehmen zu erfüllen sind.

Verzeichnis von Verarbeitungstätigkeiten
Verantwortliche und Auftragsverarbeiter müssen Verzeichnisse über ihre Verarbeitungstätigkeiten führen. Diese sollen – soweit sie ordnungsgemäß umgesetzt und aufrechterhalten werden – den Nachweis der Umsetzung der Vorgaben der

[9] Gesetz vom 30.06.2017 – BGBl. I 2017, Nr. 44 vom 05.07.2017, S. 2097.

[10] Bundesrat (2017) Beschlussdrucksache 110/17(B); Deutscher Bundestag (2017) Beschlussempfehlung; kritisch ZD 2017, 51, 51 ff.; Helfrich, ZD 2017, 97, 98; Deutscher Bundestag Online-Dienste, Kritik von Sachverständigen an geplanter Datenschutz-Novelle, abrufbar unter: https://www.bundestag.de/dokumente/textarchiv/2017/kw13-pa-innen-datenschutz-499054, zuletzt aufgerufen am: 23.11.2023.

[11] Zu der Frage der Vereinbarkeit des § 26 BDSG mit der DSGVO siehe Abschn. 8.2.2.2.

[12] Krempl, Datenschutzreform: EU-Kommission droht Deutschland mit Vertragsverletzungsverfahren, abrufbar unter: https://www.heise.de/news/Datenschutzreform-EU-Kommission-droht-Deutschland-mit-Vertragsverletzungsverfahren-3689759.html, zuletzt aufgerufen am: 23.11.2023; ZD-Aktuell 2017, 05637; zu den damaligen Bedenken gegen das BDSG siehe Helfrich, ZD 2017, 97, 98.

DSGVO gegenüber den Aufsichtsbehörden ermöglichen und zudem bei der Erfüllung von Informationspflichten gegenüber den betroffenen Personen als Hilfsmittel dienen. Die Verzeichnisse müssen unter anderem Informationen zum Verarbeitungszweck, den Kategorien der verarbeiteten personenbezogenen Daten sowie eine Beschreibung der eingesetzten technischen und organisatorischen Schutzmaßnahmen enthalten. Abschn. 3.6 enthält detaillierte Informationen zu Inhalt und Zweck der Verzeichnisse sowie zu den – in der Praxis selten anwendbaren – Ausnahmen von dieser datenschutzrechtlichen Pflicht.

Benennung eines Datenschutzbeauftragten
Privatunternehmen sind zur Ernennung eines Datenschutzbeauftragten verpflichtet, soweit ihre Kerntätigkeit – also Tätigkeiten, die für die Umsetzung der Geschäftsstrategie maßgeblich sind – in der Durchführung von Verarbeitungstätigkeiten besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen oder wenn die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten (bspw. Gesundheitsdaten) besteht. Hinzu kommen im nationalen Kontext nach dem BDSG weitere Fälle, die eine Benennungspflicht auslösen. Unternehmensgruppen steht es frei für alle oder mehrere Gruppenunternehmen einen gemeinsamen Datenschutzbeauftragten zu benennen. Der Datenschutzbeauftragte ist anhand seiner Expertise und beruflichen Qualifikation auszuwählen. Dadurch soll sichergestellt werden, dass er seine Pflichten ordnungsgemäß erfüllen kann, wie z. B. die Überwachung der Einhaltung der Vorschriften der DSGVO durch das Unternehmen. Nähere Ausführungen finden sich in Abschn. 3.10.

Datenschutz-Folgenabschätzung
Sollte eine geplante Verarbeitungstätigkeit, insbesondere unter Verwendung neuer Technologien, zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führen, müssen Unternehmen eine präventive Datenschutz-Folgenabschätzung vornehmen, um geeignete Maßnahmen zur Minimierung des Datenschutzrisikos zu ermitteln. Das Unternehmen konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus dieser Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft. Zudem erstellen und veröffentlichen die Aufsichtsbehörden künftig Listen von Verarbeitungsvorgängen (sog. „black- and whitelists“), für die eine Datenschutz-Folgenabschätzung erforderlich oder nicht erforderlich ist. Für Details zum Umfang der Datenschutz-Folgenabschätzung sowie zu den betroffenen Verarbeitungstätigkeiten siehe Abschn. 3.9.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
Die DSGVO legt einen Schwerpunkt auf präventive Datenschutzkonzepte. Da die Verpflichtung zur Berücksichtigung und Umsetzung der Prinzipien von Daten-

schutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen bußgeldbewährt ist, sollten sich Unternehmen dieser Themen ernsthaft annehmen, siehe Abschn. 3.5. Dies gilt insbesondere für solche Unternehmen, deren Kerntätigkeiten in der Verarbeitung großer Mengen personenbezogener Daten bestehen, siehe dazu Abschn. 9.1.

Technischer und organisatorischer Datenschutz
Unternehmen müssen technische und organisatorische Datenschutzmaßnahmen treffen, um die Sicherheit der von ihnen verarbeiteten personenbezogenen Daten zu gewährleisten. Das angemessene Datenschutzniveau ist im konkreten Fall anhand des Risikopotenzials der jeweiligen Datenverarbeitungstätigkeiten zu ermitteln. Einzelheiten zur Bestimmung des Risikopotenzials sowie zu den angemessenen Datenschutzmaßnahmen werden in Abschn. 3.7 dargelegt.

Rechte betroffener Personen
Betroffene Personen haben umfangreiche Informationsrechte gegenüber datenverarbeitenden Unternehmen. Letztere müssen proaktiv zahlreiche Pflichten gegenüber den betroffenen Personen erfüllen, wie etwa die Erteilung von Informationen über die Verarbeitung, das Löschen von personenbezogenen Daten oder die Berichtigung unvollständiger personenbezogener Daten. Vor allem das Recht auf Datenübertragbarkeit stellt Unternehmen vor Herausforderungen, da sie ihren Kunden auf Anfrage deren Datensätze in einem interoperablen Format zur Verfügung stellen müssen. Die Einzelheiten zu den verschiedenen Betroffenenrechten sind in Kap. 4 dargestellt.

Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen
Die DSGVO sieht eine allgemeine Meldepflicht der Verantwortlichen gegenüber den Aufsichtsbehörden für Datenschutzverletzungen (sog. „data breach notifications“) vor. Eine Datenschutzverletzung kann u. a. durch Vernichtung, Verlust oder unbefugten Offenlegung von personenbezogenen Daten verursacht werden. Die Meldung gegenüber den Aufsichtsbehörden muss regelmäßig innerhalb eines Zeitraums von 72 Stunden nach Bekanntwerden der Verletzung erfolgen. Im Falle einer Datenschutzverletzung mit hohem Risiko für die Rechte und Freiheiten der betroffenen Personen hat der Verantwortliche die Verletzung zusätzlich auch den betroffenen Personen mitzuteilen. In einem derartigen Fall werden die Aufsichtsbehörden den Verantwortlichen bei der Kommunikation unterstützen. Die Einzelheiten werden in Abschn. 3.8 dargestellt.

Datenschutzmanagement
Soweit auf Grundlage des Budgets und der Ressourcen eines Unternehmens möglich, kann die Einhaltung der Vorgaben der DSGVO mithilfe eines Datenschutz-Managementsystems sichergestellt und überwacht werden. Dabei handelt es sich um ein internes Compliance-System, welches die Erfüllung datenschutz- und sicherheitsbezogener Pflichten überprüft, siehe Abschn. 3.2.2.

Benennung eines Vertreters durch nicht in der EU niedergelassene Unternehmen
Unternehmen, auf die die DSGVO Anwendung findet, obwohl sie keine Niederlassung in der EU haben, müssen einen Vertreter in der EU benennen. Dieser soll als Anlaufstelle für betroffene Personen und Aufsichtsbehörden dienen.

Verhaltensregeln & Datenschutzzertifizierungen
Auch wenn deren Verwendung nicht verpflichtend ist, weist die DSGVO Selbstregulierungsinstrumenten, wie Verhaltensregeln und Datenschutzzertifizierungen, eine erhöhte praktische Relevanz zu. Während Verhaltensregeln die Verpflichtungen der DSGVO für einen bestimmten Sektor oder eine bestimmte Technologie präzisieren, dienen Datenschutzzertifizierungen dem Nachweis der Einhaltung der Vorgaben der DSGVO bzgl. der zertifizierten Verarbeitungstätigkeiten. Die Verwendung dieser Instrumente erleichtert den Nachweis der Einhaltung der DSGVO gegenüber den Aufsichtsbehörden, siehe Abschn. 3.12. Zudem können Unternehmen diese Instrumente als geeignete Datenschutz-Garantien für Datentransfers in Drittländer nutzen, siehe Abschn. 4.3.4.

1.2.2 Rechtmäßigkeit der Datenverarbeitung

Zusätzlich zu ihren organisatorischen Verpflichtungen nach der DSGVO müssen Unternehmen die materielle Rechtmäßigkeit ihrer Datenverarbeitungsvorgänge sicherstellen. Dies betrifft auch konzerninterne Datenverarbeitungen sowie Datentransfers in Drittländer und Verarbeitungstätigkeiten unter Einbeziehung eines Auftragsverarbeiters.

Rechtsgrundlagen für die Verarbeitung
Datenverarbeitungstätigkeiten unterliegen einem generellen Verbot mit Erlaubnisvorbehalt. Die wesentlichen der in der DSGVO vorgesehenen Rechtsgrundlagen für eine Verarbeitung waren bereits in der EG-Datenschutzrichtlinie enthalten. Die Voraussetzungen für die Einholung einer wirksamen Einwilligung der betroffenen Personen in die Datenverarbeitung wurden verschärft, wie in Abschn. 4.2.1 dargestellt. Weitere gesetzliche Erlaubnistatbestände sind, unter anderem, die Notwendigkeit der Verarbeitung zur Vertragserfüllung oder die überwiegenden berechtigten Interessen des Verantwortlichen an der Datenverarbeitung. Zudem sollten sich Unternehmen bewusst machen, dass eine Änderung des Verarbeitungszwecks nur in begrenzten Fällen zulässig ist. Einzelheiten werden in Abschn. 4.2.2.6 dargestellt.

Konzerninterne Datenverarbeitungen
Die DSGVO sieht kein Konzernprivileg vor, sodass jedes Konzernunternehmen selbst für die Einhaltung der datenschutzrechtlichen Standards im Rahmen seiner

Verarbeitungstätigkeiten verantwortlich ist. Deshalb müssen auch konzerninterne Datentransfers von einer Rechtsgrundlage gedeckt sein, grundsätzlich im gleichen Maß wie jeder Datentransfer an sonstige Dritte, siehe Abschn. 4.4.

Besondere Kategorien personenbezogener Daten
Besondere Kategorien von personenbezogenen Daten beziehen sich, unter anderem, auf politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gesundheit der betroffenen Personen. Diese Daten sind besonders schutzwürdig und ihre Verarbeitung kann nur unter Einsatz angemessener Schutzmaßnahmen erfolgen, die dem hohen Risikopotenzial der Verarbeitungssituation entsprechen. Da Beschäftigtendaten unter Umständen auch Informationen zur Gesundheit von Mitarbeitern enthalten, werden Unternehmen von diesen Einschränkungen regelmäßig betroffen sein. Dabei müssen sie beachten, dass die Verarbeitung besonderer Kategorien personenbezogener Daten verboten ist, soweit diese nicht durch die Einwilligung der betroffenen Personen oder durch die Notwendigkeit der Verarbeitung in einem Arbeits- oder Sozialversicherungskontext gerechtfertigt ist. Einzelheiten zu den verschiedenen Arten besonderer Kategorien personenbezogener Daten sowie zu den rechtlichen Grundlagen für ihre Verarbeitung sind Abschn. 4.2.3 zu entnehmen.

Auftragsverarbeitung
Die DSGVO qualifiziert den Auftragsverarbeiter nicht als Dritten. Deshalb liegt die Weitergabe personenbezogener Daten an einen Auftragsverarbeiter im freien Ermessen des Verantwortlichen und bedarf keines eigenen materiell-rechtlichen Erlaubnistatbestandes. Es ist zu beachten, dass dies auch für die Beteiligung von Auftragsverarbeitern außerhalb der EU gilt. Dabei ist der Verantwortliche zur Auswahl eines geeigneten Auftragsverarbeiters verpflichtet, welcher ein angemessenes Datenschutzniveau gewährleisten kann. In diesem Zusammenhang treffen den Auftragsverarbeiter auch eigene, bußgeldbewährte Pflichten nach der DSGVO. Einzelheiten werden in Abschn. 3.4 dargestellt.

Generelle Anforderungen an Datenübermittlungen in Drittländer
Werden personenbezogene Daten an Empfänger außerhalb der EU übermittelt, muss dieser Transfer bestimmten Garantien entsprechen, um ein angemessenes Datenschutzniveau beim Empfänger zu gewährleisten. Unternehmen müssen in zwei Stufen sicherstellen, dass die Verarbeitungstätigkeit **(i)** von einer Rechtsgrundlage gedeckt ist und **(ii)**, dass der Transfer vom Empfänger einzuhaltenden Garantien unterliegt. Die verschiedenen Garantiemechanismen sind in Abschn. 4.3 beschrieben. Aus Unternehmenssicht von hoher praktischer Relevanz sind:

EU-Standardvertragsklauseln Der unter dem Anwendungsbereich der DSGVO fallende Datenexporteur und der außerhalb der EU niedergelassene Datenimporteur können einen Vertrag auf der Grundlage von Standarddatenschutzklauseln (sog. EU-Standardvertragsklauseln) schließen. Dabei handelt es sich um Sets von Vertragsklauseln, die von der Europäischen Kommission oder einer der nationalen Auf-

sichtsbehörden verabschiedet werden. Werden die Klauseln vollständig und unverändert übernommen, dienen sie als ausreichende Garantiemaßnahme für internationale Datentransfers, siehe Abschn. 4.3.2 für Einzelheiten.

Binding Corporate Rules Konzerne oder Gruppen von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, können sich als geeignete Garantien Binding Corporate Rules auferlegen. Diese legen für die beteiligten Unternehmen eine weltweite Datenschutz-Policy im Hinblick auf Datentransfers zu Gruppenmitgliedern in Empfängerländern außerhalb der EU fest, die kein hinreichendes Datenschutzniveau vorweisen können. Ihre Wirkungsweise, ihr Mindestinhalt sowie das einzuhaltende Genehmigungsverfahren sind in Abschn. 4.3.3 beschrieben.

Transfer-Folgenabschätzung Eine umfangreiche neue Pflicht hat sich im Nachgang zum *Schrems-II*-Urteil des EuGH ergeben: die Pflicht zur Durchführung einer sog. Transfer-Folgenabschätzung (*Transfer Impact Assessment*, kurz: TIA). Datenexporteure müssen vor einer geplanten Datenübermittlung in unsichere Drittländer prüfen, ob ein vergleichbares Datenschutzniveau im Drittland besteht oder nicht. Die Transfer-Folgenabschätzung kann im Einzelfall eine große Herausforderung für Unternehmen darstellen. Wegen der Komplexität der Risikobewertung fordert eine Transfer-Folgenabschätzung einen oftmals hohen zeitlichen, finanziellen und organisatorischen Aufwand, siehe Abschn. 4.3.2. für Einzelheiten.

Referenzen

Bundesrat (2017) Beschlussdrucksache 110/17(B)
Deutscher Bundestag (2017) Beschlussempfehlung des Innenausschusses, Drucksache 18/12084
Helfrich M (2017) DSAnpUG-EU: Ist der sperrige Name hier schon Programm? ZD 7(3):97–98
Polenz S (2020) Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes. In: Taeger J, Pohle J (Hrsg) Computerrechts-Handbuch, Stand Juni 2020. C.H. Beck, München
Reiners W (2015) Datenschutz in der Personal Data Economy – Eine Chance für Europa. ZD 5(2):51–55
Ruffert M (2022) Art. 288 AEUV. In: Calliess C, Ruffert M (Hrsg) EUV/AEUV, 6. Aufl. C.H. Beck, München
Zeitschrift für Datenschutz (2017) Interview: BDSG-neu: BMI-Entwurf für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU. ZD 7(2):51–54

Anwendungsbereich der DSGVO

2

Die DSGVO enthält eine Vielzahl datenschutzrechtlicher Vorgaben, deren Nichteinhaltung sowohl für die datenverarbeitenden Stellen als auch für die Rechte und Freiheiten der betroffenen Personen mit erheblichen Risiken verbunden sein können. Zudem ist der Anwendungsbereich der DSGVO weit gefasst. Die DSGVO weist daher auch außerhalb des europäischen Raumes eine beachtliche Relevanz auf. Vor diesem Hintergrund sollten Unternehmen stets prüfen, ob die DSGVO ggf. auf sie Anwendung findet.

2.1 In welchen Fällen ist die Verordnung anwendbar? – sachlicher Anwendungsbereich

> **Artikel 2 – Sachlicher Anwendungsbereich**
> 1. Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.
>
> […]

Vereinfacht gesagt umfasst der sachliche Anwendungsbereich der DSGVO *jegliche Verarbeitungen personenbezogener Daten*. Die Verordnung wird daher für Unternehmen relevant, sobald sie Verarbeitungstätigkeiten jedweder Art vornehmen. Der (sachliche) Anwendungsbereich ist *sehr weit zu interpretieren,* um ein hohes Schutzniveau zu gewährleisten.

P. Voigt, A. von dem Bussche, *EU-Datenschutz-Grundverordnung (DSGVO)*,
https://doi.org/10.1007/978-3-662-68820-5_1

2.1.1 „Verarbeitung“

„Verarbeitung“ bezieht sich auf jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten *Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten*, Art. 4 Nr. 2 DSGVO. Praktisch jeder Umgang mit Daten wird von dieser Definition erfasst. Beispiele sind das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Offenlegung,[1] das Löschen oder die Vernichtung von Daten. Der offene Wortlaut erklärt sich aus dem Ziel des europäischen Gesetzgebers, den Anwendungsbereich unabhängig von technologischen Veränderungen zu bestimmen.[2] Er umfasst Verarbeitungen, die *ganz oder auch nur teilweise mithilfe automatisierter Verfahren* durchgeführt werden, wobei sich letzteres auf Verarbeitungen bezieht, bei denen bestimmte Verarbeitungsschritte manuell ausgeführt werden, z. B. durch die manuelle Erfassung von Daten in einem Computersystem.[3]

Beispiel

- Personenbezogene Daten werden durch den Einsatz von Computern, Smartphones, Webcams, Dashcams oder Kameradrohnen verarbeitet.
- Personenbezogene Daten werden mittels *Wearables* oder anderer *Smart Devices* (z. B. Smart Cars) erhoben.[4] ◀

Die offene Definition der „Verarbeitung“ umfasst auch kurzzeitige Nutzungen kleiner Datenmengen.[5]

Beispiel

- Personenbezogene Daten werden von einem IT-System zwischengespeichert, wie z. B. im Verlauf eines Browsers.
- Personenbezogene Daten werden auf einem Computerbildschirm angezeigt. ◀

Nichtautomatisierte Datenverarbeitung
Ausgehend von der Legaldefinition in Art. 4 Nr. 2 DSGVO ist auch die nichtautomatisierte bzw. manuelle Datenverarbeitung als „Verarbeitung“ i. S. d. DSGVO anzusehen. Im Gegensatz zu automatisierten Verarbeitungsvorgängen unter Einsatz von

[1] EuGH, Urteil vom 7. März 2024, Endemol Shine Finland Oy, C-740/22, Rn. 25 ff., in dem der Gerichtshof feststellte, dass die mündliche Weitergabe von Informationen über noch laufende oder abgeschlossene Strafverfahren gegen betroffene Personen eine Verarbeitung im Sinne der DSGVO darstellt.

[2] ErwGr. 15 DSGVO.

[3] Ernst, in: Paal/Pauly, DSGVO BDSG, Art. 2 DSGVO (2021), Rn. 6.

[4] Beispiele aus Ernst, in: Paal/Pauly, DSGVO BDSG, Art. 2 DSGVO (2021), Rn. 5–6; siehe auch EDPB, Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0 (2021a), Rn. 20; ebenfalls EDPB, Guidelines 3/2019 on processing of personal data through video devices, Version 2.0 (2020), Rn. 2.

[5] Laue, in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, § 1 Einführung (2019), Rn. 9, siehe auch für die nachfolgenden Beispiele.

Technologie wird die manuelle Verarbeitung *vollständig von Menschen ausgeführt* – ohne Einsatz von EDV-Systemen. Naturgemäß verlaufen diese Tätigkeiten wesentlich langsamer als automatisierte Verarbeitungsvorgänge, sodass deutlich geringere Datenmengen verarbeitet werden können. Deshalb unterfallen rein manuelle Datenverarbeitungen der DSGVO nur, wenn personenbezogene Daten verarbeitet werden, die in einem Dateisystem gespeichert oder gespeichert werden sollen, Art. 2 Abs. 1 DSGVO. Unter Dateisystem ist jede strukturierte Sammlung von Daten zu verstehen, welche nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird, Art. 4 Nr. 6 DSGVO. Damit ein Dateisystem im Sinne der DSGVO vorliegt müssen daher *zwei Bedingungen* erfüllt sein:

- Es muss eine strukturierte Sammlung von Daten vorliegen. Dies setzt voraus, dass mehrere Daten zusammengeführt werden. Diese Daten werden dann ausgehend von vorbestimmten Ordnungskriterien im Speichermedium in verschiedene Gruppen oder Kategorien eingeteilt und systematisch verwaltet.[6]
- Die verschiedenen Daten müssen *anhand vorbestimmter Kriterien zugänglich* sein.[7] Dies setzt voraus, dass der Zugang und die Auswertung der gespeicherten Daten nicht nur durch die Durchsicht der gesamten Datensammlung erfolgen kann, sondern der Zugang und die Auswertung von bestimmten Daten bereits durch eine Sortierung nach bestimmten Kategorien stattfinden kann.[8] Die Verordnung gibt keine Voraussetzungen bzgl. dieser Kriterien vor. Beispielsweise erfüllen chronologisch, alphabetisch oder anhand anderer Kriterien geordnete Akten diese Bedingungen.[9]

Beispiel

Eine Arztpraxis speichert ihre Patientendaten in Papierakten. Diese Akten sind alphabetisch anhand der Nachnamen der Patienten in mehreren Aktenschränken sortiert. Es gibt bspw. eine Schublade für alle Nachnamen, die mit „A" beginnen, eine für alle Nachnamen die mit „B" beginnen und so weiter.

In diesem Beispiel sind die Patientendaten alphabetisch sortiert. Dadurch sind die Daten in einem Dateisystem anhand festgelegter „Kriterien" gespeichert und fallen somit in den sachlichen Anwendungsbereich der DSGVO. ◀

Nichtautomatisierte Verarbeitung im BDSG

Während die nichtautomatisierte Datenverarbeitung nur in Ausnahmefällen in den Anwendungsbereich der DSGVO fällt, differenziert das BDSG hierbei zwischen öffentlichen und nicht öffentlichen Stellen.[10] Gem. § 1 Abs. 1 S. 2 BDSG ist das Ge-

[6] Ennöckl, in: Sydow/Marsch, DSGVO BDSG, Art. 4 DSGVO (2022), Rn. 110.

[7] Vgl. ErwGr. 15 EG-Datenschutzrichtline.

[8] Vgl. Dammann, in: Simitis, Bundesdatenschutzgesetz, § 3 BDSG (2014), Rn. 90.

[9] Plath/Struck, in: Plath, DSGVO BDSG TTDSG, Art. 2 DSGVO (2023), Rn. 12–14.

[10] Vgl. Gola/Reif, in: Gola/Heckmann, DSGVO BDSG, § 1 BDSG (2022), Rn. 4; ebenfalls Ernst, in: Paal/Pauly, DSGVO BDSG, § 1 BDSG (2021), Rn. 2–3, 5.

setz bei nichtautomatisierter Verarbeitung auf nicht öffentliche Stellen – vergleichbar mit der DSGVO – grundsätzlich nur anwendbar, wenn diese die personenbezogenen Daten in einem Dateisystem speichern bzw. speichern werden. Auf öffentliche Stellen des Bundes findet das BDSG (sowie auf öffentliche Stellen der Länder die Landesdatenschutzgesetze) hingegen ohne die vorgenannte Einschränkung Anwendung, § 1 Abs. 1 S. 1 Nr. 1 BDSG. Dies hat zur Folge, dass sich diese Einschränkung gerade nicht auf öffentliche Stellen erstreckt und mithin betroffene Personen bei jedweder Form nichtautomatisierter Verarbeitung ihrer personenbezogenen Daten durch eine öffentliche Stelle, beispielsweise in Form loser Notizzettel oder Einzeldokumente, stets durch das BDSG geschützt sind.[11]

Auch bei nicht öffentlichen Stellen sieht das BDSG in Teilen – abweichend von der allgemeinen Regelung in § 1 Abs. 2 S. 2 BDSG – eine Geltung bei nichtautomatisierter Datenverarbeitung vor. So sollen Datenverarbeitungen zu Zwecken des Beschäftigungsverhältnisses auch dann dem BDSG unterfallen, wenn die Daten nicht in einem Dateisystem gespeichert werden, § 26 Abs. 7 BDSG. Mithin unterliegt auch hier jegliche nichtautomatisierte Datenverarbeitung dem Anwendungsbereich des BDSG,[12] um einen umfassenden Schutz der Daten von Beschäftigten zu gewährleisten.

Der genaue Umfang dieser BDSG-Vorgaben bleibt aber unklar: So sollen nur die Regelungen des BDSG auf manuelle Datenverarbeitungen zur Anwendung gelangen. Das BDSG ergänzt jedoch nur die deutlich wichtigeren und umfangreicheren Regelungen der DSGVO, die in den vorgenannten Fällen weiterhin nicht zur Anwendung gelangt. Die von der DSGVO losgelöste Anwendung des BDSG wird häufig nicht sinnvoll möglich sein.

2.1.2 „Personenbezogene Daten“

Wie soeben dargelegt, fällt jeder systematische Umgang mit Daten unter den Begriff der „Verarbeitung“ i. S. d. DSGVO.[13] Der Begriff „Daten“ bezieht sich auf Informationen bzw. Einzelangaben.[14] Außerdem müssen die Daten „personenbezogen“ sein, um in den Anwendungsbereich der Verordnung zu fallen. Daten haben einen Personenbezug, soweit sie sich auf eine *identifizierte oder identifizierbare natürliche Person* beziehen, Art. 4 Nr. 1 DSGVO. Sie fallen also in den Anwendungsbereich der DSGVO, sobald die Identifizierung einer Person aufgrund der vorhandenen Daten möglich ist, was bedeutet, dass eine Person direkt oder indirekt

[11] Gola/Reif, in: Gola/Heckmann, DSGVO BDSG, § 1 BDSG (2022), Rn. 5; siehe auch Ernst, in: Paal/Pauly, DSGVO BDSG, § 1 BDSG (2021), Rn. 5.

[12] Gräber/Nolden, in: Paal/Pauly, DSGVO BDSG, § 26 BDSG (2021), Rn. 54; siehe auch Tiedemann, in: Sydow/Marsch, DSGVO BDSG, Art. 88 DSGVO (2022), Rn. 34.

[13] Barlag, in: Roßnagel, DSGVO, § 3 I. Anwendungsbereich der Datenschutz-Grundverordnung (2017), Rn. 7.

[14] Ernst, in: Paal/Pauly, DSGVO BDSG, Art. 4 DSGVO (2021), Rn. 3; siehe auch Eßer, in: Auernhammer, DSGVO BDSG, Art. 4 DSGVO (2023), Rn. 6.

mittels Zuordnung zu einem Kennungsmerkmal ermittelt werden kann. Dies ist der Fall, sobald die *Zuordnung der Daten zu einem oder mehreren Charakteristika*, die Ausdruck der physischen, physiologischen, psychischen, genetischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, möglich ist. Dabei kann es sich bspw. handeln um:

- den Namen einer Person;[15]
- Identifikationsnummern wie Sozialversicherungsnummer, Personalnummer oder Personalausweisnummer;
- Standortdaten;
- Online-Kennungen (dies kann IP-Adressen oder Cookies einschließen).[16]

Die DSGVO ist *nicht* auf die *Daten Verstorbener* anwendbar.[17] Hierbei ist aber zu beachten, dass es sich bei derartigen Daten zugleich um die personenbezogenen Daten eines lebenden Verwandten oder Nachkömmlings des Verstorbenen handeln kann.[18] Solche Daten können bspw. Aufschluss über Erbkrankheiten von Nachkommen des Verstorbenen liefern.[19] In diesem Fall unterfallen sie dem Anwendungsbereich der DSGVO.

2.1.2.1 Identifizierbarkeit der betroffenen Person

Die Identifizierung der betroffenen Person muss nicht unmittelbar anhand der Daten möglich sein, um zur Anwendbarkeit der DSGVO zu führen. Die bloße Möglichkeit der Identifizierung, also die „Identifizierbarkeit", stellt bereits einen hinreichenden Personenbezug der Daten i. S. d. DSGVO her. Die Identifizierung wird dabei erst durch die *Kombination verschiedener Informationen* möglich, die für sich allein keinen Rückschluss auf die betroffene Person zugelassen hätten, aber einen solchen in der Zusammenschau ermöglichen.[20] Der Wortlaut des Art. 4 Nr. 1 DSGVO lässt offen, wer zur Identifizierung der betroffenen Person in der Lage sein muss, was darauf hindeutet, dass zusätzliche Informationen für die Identifizierung nicht zwingend im Datenbestand des Verantwortlichen/Auftragsverarbeiters vorhanden sein müssen.

---

[15] Barlag, in: Roßnagel, DSGVO, § 3 I. Anwendungsbereich der Datenschutz-Grundverordnung (2017), Rn. 8.

[16] ErwGr. 30 DSGVO.

[17] ErwGr. 27 DSGVO.

[18] Ernst, in: Paal/Pauly, DSGVO BDSG, Art. 4 DSGVO (2021), Rn. 6; Schild, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Art. 4 DSGVO (45. Ed. 01.05.2023), Rn. 11; siehe auch Klar/Kühling, in: Kühling/Buchner, DSGVO BDSG, Art. 4 Nr. 1 DSGVO (2020), Rn. 5.

[19] Klar/Kühling, in: Kühling/Buchner, DSGVO BDSG, Art. 4 Nr. 1 DSGVO (2020), Rn. 5.

[20] Klar/Kühling, in: Kühling/Buchner, DSGVO BDSG, Art. 4 Nr. 1 DSGVO (2020), Rn. 19; vgl. EuGH, Urteil vom 7. März 2024, OC/Europäische Kommission, C-479/22 P, Rn. 64. Hier hob der EuGH eine Entscheidung des EuG auf, in der das EuG den Begriff der personenbezogenen Daten falsch ausgelegt hatte. Der EuGH stellte fest, dass eine Person durch eine Pressemitteilung identifiziert werden kann, wenn der Leser anhand der darin enthaltenen Informationen und weiterer Nachforschungen in anderen Quellen auf das Thema der Pressemitteilung schließen kann.

Relative oder absolute Kriterien

Nach ErwGr. 26 der DSGVO[21] sind zur Bestimmung der Identifizierbarkeit einer Person alle Mittel zu berücksichtigen, „die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren".[22] In diesem Zusammenhang wird diskutiert, ob relative oder absolute Kriterien[23] zur *Feststellung der Wahrscheinlichkeit einer Identifizierbarkeit* heranzuziehen sind.[24] Die Verwendung absoluter Kriterien würde dazu führen, dass die Definition „personenbezogener Daten" bereits erfüllt ist, sobald *irgendjemand die Möglichkeit zur Zuordnung* der verarbeiteten Daten zu einer natürlichen Person hat.[25]

Im Oktober 2016 entschied der EuGH, dass das tatsächliche Identifikationsrisiko unwesentlich erscheint, wenn die Zuordnung der Daten zu einem Individuum einen unverhältnismäßigen Aufwand in Bezug auf Zeit, Kosten und Personaleinsatz erfordert, wobei es sich bei den vorgenannten Faktoren um *relative Kriterien* handelt.[26] Hiernach gelten die Daten nicht als personenbezogen, wenn die Identifizierung des Betroffenen für den Verantwortlichen/Auftragsverarbeiter ausgehend von seiner Möglichkeit zum Zugriff auf zusätzliche Informationen nur mit unverhältnismäßigem Aufwand möglich ist.[27] Zwar ist das Urteil des EuGH auf Grundlage der EG-Datenschutzrichtlinie ergangen, allerdings enthält auch die DSGVO Indikatoren dafür, dass relative Kriterien maßgebend sind.[28] Daher gilt eine Person als identifizierbar, wenn die *fehlenden Informationen*, welche eine Identifizierung ermöglichen, *(leicht) zugänglich* sind, beispielsweise weil sie im Internet oder von einem (kommerziellen) Informationsdienst veröffentlicht wurden. Auch die Kenntnis Dritter von diesen Informationen ist zu berücksichtigen, sobald eine Chance besteht,

---

[21] Die Ausführungen zu relativen und absoluten Kriterien finden ihren Ursprung im Diskurs um die Auslegung des ErwGr. 26 EG-Datenschutzrichtline. Aufgrund des ähnlichen Wortlauts in der englischen Fassung des ErwGr. 26 EG-Datenschutzrichtlinie und des ErwGr. 26 DSGVO sind die zu erstere vertretenen Ansichten größtenteils auch auf die DSGVO übertragbar, laut Klar/Kühling, in: Kühling/Buchner, DSGVO BDSG, Art. 4 Nr. 1 DSGVO (2020), Rn. 20.

[22] ErwGr. 26 DSGVO.

[23] Siehe auch Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 Nr. 1 DSGVO (2019), Rn. 58–59.

[24] Für Literaturangaben zu beiden Ansichten siehe Voigt, MMR 2009, 377, 378 ff.; Bergt, ZD 2015, 365, 365 ff.

[25] Siehe auch Herbst, NVwZ 2016, 902, 904; Eßer, in: Auernhammer, DSGVO BDSG, Art. 4 DSGVO (2023), Rn. 20.

[26] EuGH, Urteil vom 19. Oktober 2016, Breyer/Bundesrepublik Deutschland, C-582/14, Rn. 39; vgl. ErwGr. 26 DSGVO.

[27] Eßer, in: Auernhammer, DSGVO BDSG, Art. 4 DSGVO (2023), Rn. 20.

[28] Hiermit ist beispielsweise der Wortlaut des ErwGr. 26 DSGVO gemeint, der die Einbeziehung verschiedener Faktoren (z. B. Zeitaufwand oder Kosten) bei der Ermittlung der wahrscheinlichen Nutzung der Mittel zur Identifizierung der Person nennt. Zustimmend siehe Eßer, in: Auernhammer, DSGVO BDSG, Art. 4 DSGVO (2023), Rn. 20; Karg; in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 Nr. 1 DSGVO (2019), Rn. 59; Piltz, K&R 2016, 557, 561; Barlag, in: Roßnagel, DSGVO, § 3 I. Anwendungsbereich der Datenschutz-Grundverordnung (2017), Rn. 9 ff.; ablehnend Buchner, DuD 2016, 155, 156.

dass der Verantwortliche/Auftragsverarbeiter Zugriff auf dieses Wissen erhält. Für die Bestimmung, ob es sich bei übermittelten Daten um personenbezogene Daten handelt, ist beispielsweise die Perspektive des Empfängers der Datenübermittlung maßgeblich.[29] So können von einem Verantwortlichen gespeicherte dynamische IP-Adressen personenbezogene Daten der betroffenen Person sein, sofern dem Verantwortlichen bspw. rechtliche Mittel zur Verfügung stehen, die vernünftigerweise eingesetzt werden können, um mithilfe Dritter (Internetzugangsanbietern oder zuständigen Behörden) die betreffende Person anhand der gespeicherten IP-Adressen bestimmen zu lassen.[30] Des Weiteren kann auch eine Fahrzeug-Identifizierungsnummer[31] (sog. FIN), welche isoliert bloß ein sachbezogenes Merkmal darstellt, gegebenenfalls einen Personenbezug aufweisen, wenn der Verantwortliche, der Zugang zu der FIN hat, auch über Mittel verfügt, die es ihm ermöglichen, eine natürliche Person in Verbindung mit der FIN zu identifizieren (bspw. durch Zugriff auf eine Zulassungsbescheinigung für den Fall, dass der Halter auch eine natürliche Person ist).[32] Im Umkehrschluss: sobald keine realistische Chance besteht, dass der Verantwortliche/Auftragsverarbeiter Zugriff auf die Information erlangt, gilt eine Person nicht als identifizierbar.

Umstände des Einzelfalls

Um eine Identifizierbarkeit zu beurteilen, sind des Weiteren die Umstände des Einzelfalls zu berücksichtigen. Dies bezieht sich u. a. auf:[33]

- die für die Identifizierung notwendigen *zeitlichen und monetären Mittel*;
- die zum Verarbeitungszeitpunkt verfügbare Technologie sowie *technologische Entwicklungen*;
- den *Zweck der Verarbeitung*.

Ist der Verarbeitungszweck nur über eine Identifikation der betroffenen Personen erreichbar, kann unterstellt werden, dass der Verantwortliche/Auftragsverarbeiter über die Mittel zur Identifizierung dieser Betroffenen verfügt.[34] Kurz gesagt, je einfacher und schneller eine natürliche Person ermittelt werden kann, desto eher handelt es sich um eine „identifizierbare natürliche Person".[35]

---

[29] EuG, Urteil vom 26. April 2023, SRB/EDSB, T-557/20, Rn. 99 ff.

[30] BGH, Urteil vom 16. Mai 2017, VI ZR 135/13, Rn. 24; zur Einordnung des TC-Strings als personenbezogene Daten aufgrund der Möglichkeit der Identifizierung eines Nutzers u. a. über die IP-Adresse siehe EuGH, Urteil vom 7. März 2024, IAB Europe/Gegevensbeschermingsautoriteit, C-604/22, Rn. 32 ff.

[31] Die FIN stellt einen alphanumerischen Code dar, welches es erlaubt, den Hersteller eines Fahrzeuges zu identifizieren.

[32] EuGH, Urteil vom 9. November 2023, Gesamtverband Autoteile-Handel e. V./Scania CV AB, C-319/22, wobei der EuGH die bereits bekannten Maßstäbe aus dem Breyer-Urteil (C-582/14) für die DSGVO bestätigte. Das Gericht ließ aber weiterhin offen, unter welchen Voraussetzungen ein Mittel „vernünftigerweise" zur Identifizierung einer Person eingesetzt werden könne.

[33] ErwGr. 26 DSGVO.

[34] Siehe auch Art. 29 Datenschutzgruppe, WP 136 (2007), S. 18 ff.

[35] ErwGr. 26 DSGVO.

2.1.2.2 Anonymisierung und Pseudonymisierung

Anonymisierung

Anonymisierung ist eine Technik zur *Veränderung* personenbezogener Daten mit dem Ergebnis, dass *keine Verbindung* der Daten *zu einer natürlichen Person (mehr) besteht*. Anonymisierte Daten sind Informationen, die entweder keinen Bezug zu einer identifizierten oder identifizierbaren Person haben, oder es handelt sich um personenbezogene Daten, bei denen der Personenbezug aufgrund einer durchgeführten Anonymisierung nicht mehr besteht.[36] Die Anonymisierung kann durch eine Reihe verschiedener *Techniken* erreicht werden, die in der Regel in eine der *beiden nachfolgenden Kategorien* fallen:

1. *Randomisierung*: Diese Technik besteht in der Veränderung der Genauigkeit von Daten, um die starke Verbindung zwischen den Daten und der betroffenen Person zu entfernen (u. a. mithilfe von Zufallsgrößen, bspw. wenn Körpergrößen nicht auf den Zentimeter genau, sondern um ca. 10 cm mehr oder weniger angegeben werden).[37] Werden die Daten hinreichend ungenau bzw. unzuverlässig, können sie nicht mehr einer bestimmten Person zugeordnet werden.[38]
2. *Generalisierung*: Diese Technik besteht in der Verallgemeinerung/Verwässerung der Merkmale der betroffenen Personen, indem der entsprechende Bezugspunkt oder die Reihenfolge der Daten verändert werden (z. B. Bezug der Daten zu einer Region anstelle einer Stadt, zu einem Monat anstelle einer Woche).[39]

Im Falle einer erfolgreichen Anonymisierung ist die DSGVO *nicht anwendbar*.[40] Derartige Techniken werden häufig im Zusammenhang mit statistischen oder Forschungszwecken angewandt. Sobald der Verantwortliche/Auftragsverarbeiter die anonymisierten Informationen allerdings mit hinreichender Wahrscheinlichkeit wiederherstellen kann, handelt es sich um personenbezogene Daten im Anwendungsbereich der DSGVO.

Beispiel

Für sein anstehendes zwanzigstes Jubiläum möchte ein privater Nachhilfeanbieter herausfinden, wie viele seiner bisher betreuten Schüler eine Universität besucht haben und, sofern dies der Fall war, was sie studiert haben. Zu diesem Zweck erhebt der Anbieter die Daten seiner Nachhilfeschüler der vergangenen 20 Jahre und kontaktiert diese via E-Mail, in welcher um die Teilnahme an einer Online-Befragung gebeten wird. Um die Daten der betroffenen Personen zu anonymisieren enthält die Umfrage keine Fragen zu Namen, E-Mail-Adressen,

[36] ErwGr. 26 DSGVO.

[37] Arning/Rothkegel, in: Taeger/Gabel, DSGVO BDSG TTDSG, Art. 4 DSGVO (2022), Rn. 50.

[38] Siehe auch Art. 29 Datenschutzgruppe, WP 216 (2014), S. 12.

[39] Siehe auch Art. 29 Datenschutzgruppe, WP 216 (2014), S. 16; siehe auch Hansen, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 Nr. 5 DSGVO (2019), Rn. 54.

[40] ErwGr. 26 DSGVO.

Abschlussjahrgängen oder Geburtsdaten der Teilnehmer. Deren IP-Adressen werden außerdem bei der Teilnahme nicht gespeichert. Um zudem die Identifizierung ehemaliger Nachhilfeschüler, die in ungewöhnlicheren Studienfächern ihren Abschluss gemacht haben, aufgrund dieser Informationen zu verhindern, werden Studienfächer nicht gesondert abgefragt, sondern lediglich verschiedene Studienfelder erfasst, bspw. „Naturwissenschaften", „Rechts- und Wirtschaftswissenschaften", „Sozial- und Erziehungswissenschaften" und „Sprach- und Kulturwissenschaften".[41]

In diesem Beispiel versucht der Nachhilfeanbieter die Erfassung von Informationen zu vermeiden, die eine Identifizierung einzelner Umfrage-Teilnehmer ermöglichen, z. B. aufgrund ihres Namens, Geburtsdatums oder sogar ungewöhnlicher Studienfächer. Durch die Reduzierung der erfassten Menge an Daten auf das notwendige Minimum zur Auswertung der Umfrage sowie das Nicht-Speichern der IP-Adressen ist die Wahrscheinlichkeit einer Re-Identifizierung der Teilnehmer verschwindend gering. Deshalb ist die Anonymisierung der Daten erfolgreich und die DSGVO findet keine Anwendung. ◀

Vorteile der Anonymisierung

Die Anonymisierung bietet eine Reihe von Vorteilen für den Verantwortlichen/Auftragsverarbeiter. Unternehmen sammeln und speichern häufig große (manchmal sogar exzessive) Datenmengen, obwohl sie letztlich nur einen kleinen Teil der Datenmenge für ihre Verarbeitungstätigkeiten benötigen. Die *Nicht-Erfassung oder Löschung* der überschüssigen Daten kann dabei helfen, eine Anonymisierung der Daten herbeizuführen, um so die Anwendbarkeit der DSGVO zu verhindern. In Bezug auf die Verarbeitung rein anonymer Daten unterliegt der Verantwortliche/Auftragsverarbeiter nicht den verschiedenen Datenschutzverpflichtungen der Verordnung (siehe Kap. 3). Zusätzlich kann eine derartige *Datenminimierung* Zeit, Kosten und personelle Ressourcen einsparen. Unternehmen sollten den Einsatz von Anonymisierungstechniken in Betracht ziehen, damit die Anwendbarkeit der DSGVO und dementsprechend auch das Risiko eines bußgeldbewährten Datenschutzverstoßes minimiert werden kann.

Praxishinweise[42]

Da sich der europäische Gesetzgeber nicht zu den Standards für eine erfolgreiche Anonymisierung geäußert hat, ist zur Verbesserung der Datensicherheit eine Kombination von Randomisierungs- und Verallgemeinerungstechniken ratsam.

Da der Anonymisierung stets ein *Risikofaktor* anhaftet, muss dieser bei der Bewertung verfügbarer Anonymisierungstechniken entsprechend der Schwere und Wahrscheinlichkeit des identifizierten Risikos Berücksichtigung finden. Als Konsequenz daraus ergibt sich, dass die optimale Anonymisierungslösung stets auf

[41] Siehe auch Dammann, in: Simitis, Bundesdatenschutzgesetz, § 3 BDSG (2014), Rn. 201 ff.

[42] Für die nachfolgenden Praxishinweise siehe auch Art. 29 Datenschutzgruppe, WP 216 (2014), S. 6, 7, 12, 16, 23–25

Einzelfallbasis zu bestimmen ist. Dies schließt eine *Bewertung des Verarbeitungskontextes* ein: „alle" Mittel, die „vernünftigerweise" für eine Re-Identifikation zur Verfügung stehen, müssen Berücksichtigung finden. Sobald die optimale Anonymisierungslösung gefunden ist, erfordert ihre Anwendung eine sorgfältige technische Implementierung, um die Widerstandsfähigkeit der technologischen Umsetzung zu erhöhen. Auch nach ihrer Anwendung bedarf die Anonymisierungstechnik einer *durchgehenden Überwachung*,[43] um dem ihr inhärenten Risikopotenzial effektiv zu begegnen, vor allem was das Identifizierungsrisiko bzgl. nicht-anonymisierter Teile der Datenbank betrifft. Mangels hinreichender Ausgestaltung des Begriffs der Anonymisierung durch den europäischen Gesetzgeber ist es schwierig abzuschätzen, welche Maßnahmen genau eine erfolgreiche Anonymisierung gewährleisten. Folglich ist die Aussage, Daten seien anonym, häufig kritisch zu hinterfragen. Da die Anonymisierung eine Methode zur Verarbeitung personenbezogener Daten darstellt, bedarf sie nach häufig vertretener Ansicht einer Rechtsgrundlage, wobei hierbei in vielen Fällen eine Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f DSGVO in Betracht kommen dürfte.[44]

Pseudonymisierung
Pseudonymisierung ist in der Praxis ein gebräuchliches Mittel, um die Möglichkeit zur Identifikation betroffener Personen anhand ihrer Daten zu vermeiden. Es handelt sich um die Verarbeitung personenbezogener Daten in einer Weise, in der die Daten *ohne Hinzuziehung zusätzlicher Informationen nicht mehr* einer *spezifischen betroffenen Person zugeordnet* werden können, Art. 4 Nr. 5 DSGVO. Dies kann erreicht werden, indem der Name des Betroffenen oder andere Merkmale durch bestimmte Angaben ersetzt werden. Die zusätzlichen Informationen, die eine Identifizierung möglich machen würden, müssen *gesondert aufbewahrt* werden. Außerdem muss die Pseudonymisierung durch den Einsatz technischer und organisatorischer Mittel zusätzlich gesichert werden. Dies kann über eine *Verschlüsselung* der Daten erreicht werden, wobei der Schlüssel nur wenigen Personen mitgeteilt wird.[45]

Es muss beachtet werden, dass, im Gegensatz zu anonymisierten Daten, pseudonymisierte Daten noch in den *Anwendungsbereich der DSGVO* fallen, da das Risiko einer Re-Identifikation höher ist als bei anonymisierten Daten. Nichtsdestotrotz handelt es sich bei der Pseudonymisierung um eine Möglichkeit für Verantwortliche und Auftragsverarbeiter, ihre Datenschutzverpflichtungen nach der DSGVO zu erfüllen und deren Einhaltung so auch nachzuweisen:[46]

---

[43] BfDI, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche (2020), S. 11.

[44] BfDI, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche (2020), S. 5, 11.

[45] Klar/Kühling, in: Kühling/Buchner, DSGVO BDSG, Art. 4 Nr. 5 DSGVO (2020), Rn. 9, 10.

[46] ErwGr. 28 DSGVO; Laue, in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, § 1 Einführung (2019), Rn. 25–26, 28; siehe letztere auch für die nachfolgenden Ausführungen.