ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Wichtige Begriffe des Datenschutzrechts

Eine Arbeitshilfe für Start-Ups

Autoren

Linda Schreiber
Annika Selzer

Impressum

Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
c/o Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Rheinstraße 75
64295, Darmstadt

Hinweise

Dieser Beitrag wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16KIS0921(Gründungsinkubator StartUpSecure) gefördert. Darüber hinaus wurde der Beitrag vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

Inhalt

1. Motivation des Dokuments

Für Start-Ups ist die Umsetzung rechtlicher Anforderungen häufig eine Mammutaufgabe, die an Kindheitstage erinnert: Einerseits schon „groß genug", um rechtliche Anforderungen umsetzen zu müssen, andererseits noch „zu klein" um über eigenes rechtliches Know-How zu verfügen bzw. eine entsprechende Fachkraft einstellen zu können. Vor diesem Hintergrund sind Start-Ups auf Arbeitshilfen angewiesen, die ihnen die für sie wichtigsten rechtlichen Anforderungen aufzeigen und erläutern. Zwei derartige Arbeitshilfen wurden im Rahmen von Start Up Secure ATHENE bereits veröffentlicht, nämlich:

- eine Checkliste, die Fragen zum Umsetzungsstand wichtiger rechtlicher Anforderungen enthält (www.athene-center.de/checkliste-startups)
  und
- ein Whitepaper, das diese rechtlichen Anforderungen näher beleuchtet und die für die Umsetzung wichtigsten Schritte erläutert (www.athene-center.de/compliance-whitepaper).

Ein wichtiger Fokus der vorgenannten Arbeitshilfen ist die Beleuchtung der datenschutzrechtlichen Anforderungen, die Start-Ups erfüllen müssen – also eine Übersicht über diejenigen rechtlichen Pflichten, die im Zusammenhang mit der Verarbeitung sogenannter personenbezogener Daten stehen. Wie viele andere Rechtsgebiete hat das Datenschutzrecht gewissermaßen seine eigene Sprache, die insbesondere durch Begriffsbestimmungen der Datenschutz-Grundverordnung (DSGVO) – dem zentralen Europäischen Rechtsakt zur Regelung des Datenschutzes – geprägt wird. Um eine weitere Arbeitshilfe für Start-Ups zu schaffen, datenschutzrechtliche Anforderungen besser verstehen zu können, hat es sich das vorliegende Dokument zur Aufgabe gemacht, wichtige Begriffe des Datenschutzrechts im Detail zu erläutern.

Das Dokument ist in Form eines Glossars aufgebaut, wobei sich die Reihenfolge der Begriffserklärungen nach Art. 4 DSGVO richtet, der (kurze) Definitionen der Begriffe enthält.[1]

2. Glossar des Datenschutzrechts

2.1. Personenbezogene Daten

Das **personenbezogene Datum** stellt den zentralen Begriff des Datenschutzrechts dar. Laut Legaldefinition des Art. 4 Nr. 1 DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare **natürliche** Person („betroffene Person") beziehen. Die Voraussetzung „alle Informationen" ist in diesem Zusammenhang weit zu verstehen und kann neben objektiven Informationen und nachprüfbaren Angaben (zum Beispiel Geburtsdatum, Adresse oder Körpergröße) auch subjektive Informationen (zum Beispiel Einschätzungen, Werturteile oder Meinungen) sowie statistische Prognosewerte einschließen.[2] Personenbezogene Daten **juristischer Personen** fallen regelmäßig nicht unter den Schutzumfang der Datenschutz-Grundverordnung, was auch aus Erwgr. 14 hervorgeht. Dieser besagt, dass die Datenschutz-Grundverordnung nicht für die Verarbeitung

[1] Der vorliegende Beitrag ist ursprünglich im Jahr 2018 erschienen als Selzer in Jandt/Steidle, Begriffsbestimmungen, Datenschutz im Internet, Nomos-Verlag und wurde für die hier erfolgende Veröffentlichung aktualisiert.
[2] Kühling/Buchner/Klar/Kühling DSGVO Art. 4 Rdnr. 8 ff.; Selzer/Diel/Schreiber DSGVO Art. 4 Rdnr. 3.

personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person gilt. Dieser Hinweis führt dazu, dass die Datenschutz-Grundverordnung auch dann nicht ihren Schutz entfaltet, wenn zum Beispiel die Kontaktdaten eines Unternehmens natürliche Personen benennen.[3]

Nur eine natürliche Person kann **betroffene Person** im Sinne der Datenschutz-Grundverordnung sein. Dabei ist nach Erwgr. 14 ihre Staatsangehörigkeit oder ihr Aufenthaltsort unerheblich. Der Schutz natürlicher Personen umfasst nur den Schutz lebender Personen und laut Erwgr. 27 ausdrücklich nicht den Schutz Verstorbener,[4] wobei die Mitgliedstaaten Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen können, so zum Beispiel in Deutschland § 203 Abs. 5 StGB. Bei der Frage, ob es sich bei einem Datum um ein personenbezogenes Datum handelt, ist das Merkmal der **Identifizierbarkeit** besonders relevant. Eine Person ist laut der Legaldefinition aus Art. 4 Nr. 1 DSGVO dann als identifizierbar anzusehen, wenn sie **mittels Zuordnung** zu einer Kennung oder zu einem oder mehreren besonderen Merkmalen **direkt oder indirekt identifiziert** werden kann.

Eine **Kennung** kann laut Legaldefinition unter anderem ein Name, eine Kennnummer, Standortdaten und eine Online-Kennung sein. Ein Beispiel für eine **Online-Kennung** ist eine **IP-Adresse**. Nach Erwgr. 30 werden natürlichen Personen unter Umständen Online- und Cookie-Kennungen sowie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren. Besondere Merkmale sind laut Legaldefinition Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität einer natürlichen Person sind.

Für die Auslegung des Begriffs der **Identifizierbarkeit** gibt es nach dem bislang geltenden Recht zwei Theorien: Die **relative Theorie** besagt, dass es für die Identifizierbarkeit einer Person ausschließlich auf die Kenntnisse der datenverarbeitenden Stelle ankommt. Die **absolute Theorie** besagt hingegen, dass es für die Identifizierbarkeit einer Person nicht nur auf die Kenntnisse der datenverarbeitenden Stelle ankommt, sondern darauf, dass irgendein Dritter das Zusatzwissen zur Identifizierbarkeit der Person besitzt.[5] Laut Erwgr. 26 sollten, um festzustellen, ob eine natürliche Person identifizierbar ist, alle Mittel berücksichtigt werden, die von dem Verantwortlichen **oder einer anderen Person** nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.

Bei der Feststellung, ob Mittel **nach allgemeinem Ermessen wahrscheinlich** zur Identifizierung der natürlichen Person genutzt werden, sollten alle **objektiven Faktoren**, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden. Hierbei sind die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen. Eine

[3] S. kritisch dazu, dass Adressdaten juristische. Personen mit personellen Komponenten nicht von der DSGVO erfasst werden Gola /Heckmann/Gola DSGVO Art. 4 Rdnr. 26.

[4] Immer wieder kommt es vor, dass Hinterbliebene Einträge der Verstorbenen, z.B. in Blogs und auf Social Media Plattformen, löschen lassen möchten oder Zugriff auf diese und auf E-Mails erhalten möchten, weil sie sich von dem Zugriff z.B. Informationen über die Umstände des Todes versprechen. Dies kann in der Praxis mit Schwierigkeiten verbunden kann. Grundsätzlich hat hierzu aber der BGH im Jahr 2018 entschieden, dass der Zugang zu Social Media Accounts oder E-Mail-Konten und den darin vorgehaltenen Kommunikationsinhalten auf die Erben übergeht und das postmortale Persönlichkeitsrecht, das Fernmeldegeheimnis oder das Datenschutzrecht dem nicht entgegenstehen, BGH Urt. v. 12.7.2018 Az. III ZR 183/17.

[5] Roßnagel/Husemann 2018, 84 f.; Kühling/Buchner/Klar/Kühling DSGVO Art. 4 Nr. 1 Rdnr. 25 ff.; Finck/Pallas International Data Privacy Law 2020, 11 (17).

besondere Betonung sollte hierbei auf die Formulierung „nach allgemeinem Ermessen wahrscheinlich" gelegt werden, wodurch der ggf. bestehende erste Eindruck, die Datenschutz-Grundverordnung folge der absoluten Theorie der Identifizierbarkeit, in dem Sinne relativiert wird, dass nur diejenigen Mittel bei der Frage der Identifizierbarkeit zu berücksichtigen sind, die von dem Verantwortlichen, aber auch einer anderen Person, im konkreten Fall **wahrscheinlich** genutzt werden.[6] Geht man davon aus, dass bei strenger Auslegung der absoluten Theorie und Heranziehung allen verfügbaren Wissens bei allen möglichen Dritten praktisch jedes Datum einer Person zugeordnet werden kann, würde das Kriterium der Personenbeziehbarkeit seine Eignung zur Differenzierung gegenüber nicht personenbeziehbaren Daten verlieren, für die das Datenschutzrecht keine Anwendung findet. Eine solche Konturlosigkeit des zentralen Begriffs der Personenbeziehbarkeit wäre der Systematik des Datenschutzrechts fremd. Im Ergebnis ist daher der relativen Theorie der Identifizierung zu folgen.

Häufig behandelt wurde im Zusammenhang mit der **Identifizierbarkeit** auch die Frage, ob **IP-Adressen** personenbezogene Daten im Sinne der Legaldefinition darstellen. Vor allem bei dynamischen IP-Adressen wurde lange Zeit diskutiert, ob diese nur für den Access-Provider oder auch für Webseiten-Betreiber ein personenbezogenes Datum darstellen.[7] Der Webseiten-Betreiber weiß in der Regel nicht, welche natürliche Person sich hinter einer IP-Adresse verbirgt, während der Access-Provider die Information, welcher natürlichen Person er welche IP-Adresse zugeordnet hat, kennt, sie jedoch nur in Ausnahmefällen herausgeben darf.[8] Der Europäische Gerichtshof vertritt hierzu die Auffassung , dass eine dynamische IP-Adresse für den Betreiber einer Webseite zumindest dann ein personenbezogenes Datum darstellt, wenn der Betreiber über rechtliche Mittel verfügt, mit deren Hilfe er die betroffene Person identifizieren lassen kann.[9] Das ist in der Regel der Fall, beispielsweise im Falle einer Auflösung mittels gerichtlicher Hilfe bei Urheberrechtsverletzungen. Dieses weite Verständnis der Identifizierbarkeit legt auch **Erwgr. 30** nahe, in dem IP-Adressen ohne Unterscheidung nach dynamischen oder statischen IP-Adressen als Beispiele für Online-Kennungen im Sinne der der Legaldefinition aus Art. 4 Nr. 1 DSGVO genannt werden.

Zu den „**besonderen Kategorien personenbezogener Daten**" zählen nach Art. 9 Abs. 1 DSGVO Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Für diese Datenkategorien gilt nach Art. 9 Abs. 1 DSGVO ein grundsätzliches Verarbeitungsverbot. Dieses wird nach Erwgr. 51 damit begründet, dass personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, einen besonderen Schutz verdienen, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten betroffener Personen auftreten können. Jedoch sind Ausnahmen in Art. 9 Abs. 2 DSGVO von dem allgemeinen Verbot der Verarbeitung besonderen Kategorien personenbezogener Daten ausdrücklich vorgesehen, unter anderem bei ausdrücklicher **Einwilligung** der

[6] S. auch Hofmann/Johannes ZD 2017, 221 (224), die zur Frage der relativen Theorie ausführen: „[….] Der Verantwortliche oder die andere Person dürften einen übermäßigen Aufwand in einem für sie unbedeutenden Fall vernünftigerweise nicht auf sich nehmen. [….] Die Wahrscheinlichkeit variiert folglich je nach Bezugsperson und spricht für ein relatives Verständnis des Personenbezugs."

[7] S. hierzu u.a. Simitis/Dammann BDSG § 3 Rdnr. 63; Steidle/Pordesch DuD 2008, 324 (327).

[8] Diese Situation ist nicht grds. anders, als bspw. bei Bankverbindungen oder Kfz-Kennzeichen, bei denen zur Identifizierung i.d.R. auch das Wissen Dritter herangezogen werden muss.

[9] EuGH, Urteil vom 19.10.2016 – C-582/14.

betroffenen Person oder bei bestimmten Notwendigkeiten, insbesondere wenn die Verarbeitung im Rahmen rechtmäßiger Tätigkeiten bestimmter Vereinigungen oder Stiftungen vorgenommen wird, die sich für die Ausübung von Grundfreiheiten einsetzen.

Rein formal handelt es sich bei **personenbezogenen Daten von Kindern nicht** um besondere Kategorien personenbezogener Daten. Gleichwohl gilt es zu beachten, dass der Europäische Gesetzgeber an deren Verarbeitung nach Art. 8 DSGVO ebenfalls besondere Bedingungen knüpft und dies in Erwgr. 38 damit begründet, dass Kinder im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten einen besonderen Schutz verdienen. Dies ergibt sich insbesondere daraus, dass Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind.

2.2. Verarbeitung und Einschränkung der Verarbeitung

Der Begriff der „Verarbeitung" stellt einen weiteren zentralen Begriff des Datenschutzrechtes dar. Nach Art. 4 Nr. 2 DSGVO umfasst die Verarbeitung jeden ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten - mit oder ohne Hilfe automatisierter Verfahren. Grundvoraussetzung für eine Verarbeitung ist also zunächst, dass personenbezogene Daten von dem Verarbeitungsvorgang betroffen sind. Ein Verarbeitungsvorgang kann sowohl **technisch-automatisiert** als auch **manuell** erfolgen. Dabei ist der sachliche Anwendungsbereich der Datenschutz-Grundverordnung nach Art. 2 Abs. 1 DSGVO auf die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, beschränkt. Zudem müssen ein Vorgang oder eine Vorgangsreihe ausgeführt werden. Das Wort „Ausführen" macht deutlich, dass der Vorgang eines menschlichen Handelns bedarf. Auch das Initiieren einer automatisieren Verarbeitung durch ein menschliches Handeln fällt hierunter.[10]

Unter den Begriff der Verarbeitung fallen nach Art. 4 Nr. 2 DSGVO insbesondere 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. Einige dieser Begriffe wurden bereits vor in Kraft treten der DSGVO in der bis 2018 gültigen alten Fassung des Bundesdatenschutzgesetzes (BDSG aF) verwendet und definiert.
Unter dem **Erheben** ist gemäß § 3 Abs. 3 BDSG a.F. das Beschaffen von Daten über den Betroffenen zu verstehen. Durch das Erheben gelangen personenbezogene Daten erstmalig in den Verfügungsbereich des Verantwortlichen.[11] Eine Beschaffung personenbezogener Daten hat gezielt, zum Beispiel durch das Anfordern von Unterlagen, zu erfolgen. Die Art und Weise der Erhebung ist insofern nicht ausschlaggebend. Werden dem Verantwortlichen personenbezogene Daten allerdings ohne dessen gezieltes Zutun, zum Beispiel zufällig oder ohne vorherige Anforderung, verfügbar, so fällt dieser Vorgang regelmäßig nicht unter den Begriff der Erhebung. Gleichwohl ist davon auszugehen, dass die Daten in der Folge einer ohne gezieltes Zutun erfolgten Kenntnisnahme durch den Verantwortlichen erfasst oder gespeichert werden.[12]

[10] Kühling/Buchner/Herbst DSGVO Art. 4 Nr. 2 Rdnr. 14.
[11] Kühling/Buchner/Herbst DSGVO Art. 4 Nr. 2 Rdnr. 21.
[12] Paal/Pauly/Ernst DSGVO Art. 4 Rdnr. 23.

Durch das **Organisieren und Ordnen** soll personenbezogenen Daten eine Struktur verliehen werden, um diese beispielsweisebesser auffinden und/oder auswerten zu können.[13]

Das **Erfassen** ist als ein Unterbegriff des Speicherns zu verstehen. Dies war deutlich nach § 3 Abs. 4 Nr. 1 BDSG aF, wonach **Speichern** das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung ist. An diesem Verständnis hat sich nichts geändert. Für das Speichern ist es nicht erforderlich, dass der Verantwortliche Besitzer des Datenträgers ist, so dass ein Speichervorgang auch dann vorliegt, wenn dieser zum Beispiel in dem Rechenzentrum eines Auftragsverarbeiters im Rahmen der Bereitstellung eines Cloud Computing Services vorgenommen wird.[14] Werden Informationen auswendig gelernt und sind somit ausschließlich im menschlichen Gedächtnis vorhanden, ist kein Speichervorgang im datenschutzrechtlichen Sinne erfüllt.[15]

Anpassung und Veränderung bedeuten gemäß § 3 Abs. 4 Nr. 2 BDSG a.F. das inhaltliche Umgestalten gespeicherter personenbezogener Daten. Bei einer Anpassung werden Daten zum Beispiel an aktuelle Gegebenheiten angepasst und somit aktualisiert, so zum Beispiel bei der jährlichen Fortschreibung des Alters in einem Datenbestand. Eine Veränderung erfolgt hingegen zum Beispiel dann, wenn eine unrichtige Altersangabe in einem Datenbestand korrigiert wird.[16]

Als **Auslesen** wird das Zurückgewinnen von Informationen aus einem vorhandenen Datensatz, also bereits gespeicherten Daten, verstanden. Das **Abfragen** ist als Unterbegriff des Auslesens zu verstehen, bei dem die Informationen aus einem vorhandenen Datensatz, zum Beispiel durch die Eingabe von Suchbegriffen, zurückgewonnen werden.[17]

Eine **Verwendung**[18] personenbezogener Daten liegt gemäß § 3 Abs. 5 BDSG a.F. vor, soweit es sich nicht um eine Verarbeitung handelt. Wie bereits im Bundesdatenschutzgesetz a.F. handelt es sich um einen Auffangtatbestand mit dem Ziel zu definieren, dass jeder Umgang mit personenbezogenen Daten in den Anwendungsbereich der Datenschutz-Grundverordnung fallen soll, auch wenn dieser nicht in den übrigen Verarbeitungsarten des Art. 4 Nr. 2 DSGVO erfasst ist. Diese Auffassung legt auch die englische Fassung der Datenschutz-Grundverordnung nahe, in der die Verwendung als „use" bezeichnet wird.

Unter dem Begriff der **Offenlegung** im Sinne der Datenschutz-Grundverordnung sind alle Vorgänge gebündelt, durch die ein Verantwortlicher personenbezogene Daten anderen Stellen zugänglich macht. Unter **Verbreitung** wird regelmäßig die weitläufig erreichbare Veröffentlichung personenbezogener Daten, etwa in einem Internet-Forum oder einem Weblog, zu verstehen sein.[19]

Ein **Abgleich** von Daten erfolgt entweder durch die reine Überprüfung, ob ein personenbezogenes Datum in zwei oder mehreren Dateisystemen gleichzeitig gespeichert ist oder durch die Kontrolle der Konsistenz der relevanten Daten, die in zwei oder mehreren Dateisystemen gespeichert sind. Demgegenüber bedeutet die **Verknüpfung** eine Zusammenführung personenbezogener Daten aus

[13] Kühling/Buchner/Herbst DSGVO Art. 4 Nr. 2 Rdnr. 23.
[14] Kühling/Buchner/Herbst DSGVO Art. 4 Nr. 2 Rdnr. 24.
[15] Paal/Pauly/Ernst DSGVO Art. 4 Rdnr. 24.
[16] Paal/Pauly/Ernst DSGVO Art. 4 Rdnr. 27.
[17] Kühling/Buchner/Herbst DSGVO Art. 4 Nr. 2 Rdnr. 27.
[18] Im BDSG a.F. wurde die Verwendung iSd DSGVO als Nutzen bezeichnet.
[19] Kühling/Buchner/Herbst DSGVO Art. 4 Nr. 2 Rdnr. 32.

mehreren Dateisystemen. Hierbei kann es sich sowohl um die Verknüpfung personenbezogener Daten zu einer betroffenen Person, als auch um die Verknüpfung mehrerer betroffener Personen handeln, wenn diese zum Beispiel ein verbindendes Merkmal innehalten und dies durch die Verknüpfung zum Ausdruck gebracht werden soll.[20]

Das **Löschen** ist gemäß § 3 Abs. 4 Nr. 5 BDSG a.F. das Unkenntlichmachen gespeicherter personenbezogener Daten. Dies kann unter anderem durch das Überschreiben von Daten auf einem Datenträger erreicht werden, wodurch sichergestellt wird, dass die ursprünglich auf dem Datenträger enthaltenen Informationen nicht mehr wiederhergestellt und somit wahrgenommen werden können. Im Internet kann das Löschen von Daten mit besonderen Schwierigkeiten verbunden sein.

Das **Vernichten** ist eine Form des Löschens, wobei sich das Vernichten auf das physische Zerstören eines Datenträgers bezieht. Auch bei der Vernichtung sollen Informationen nach dem Vorgang der Vernichtung nicht mehr wiederherstellbar und wahrnehmbar sein. Vernichtet werden können zum Beispiel Papierakten und Festplatten.[21]

Unter einer **Einschränkung der Verarbeitung**, die auch Bestandteil der Begriffsdefinition der Verarbeitung in Art. 4 Nr. 2 DSGVO ist, versteht man gemäß Art. 4 Nr. 3 DSGVO die **Markierung** gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken, was der Bezeichnung der Datensperrung gleichkommt. Laut Erwgr. 67 können Methoden zur Beschränkung der Verarbeitung personenbezogener Daten unter anderem darin bestehen, dass ausgewählte personenbezogenen Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden, dass sie für Nutzer gesperrt werden oder dass veröffentliche Daten vorübergehend von einer Website entfernt werden. In automatisierten Dateisystemen sollte die Einschränkung der Verarbeitung grundsätzlich durch technische Mittel so erfolgen, dass die personenbezogenen Daten in keiner Weise weiterverarbeitet werden und nicht verändert werden können. Auf die Tatsache, dass die Verarbeitung der personenbezogenen Daten beschränkt wurde, sollte in dem System unmissverständlich hingewiesen werden. Gemäß Art. 18 Abs. 2 DSGVO dürfen personenbezogenen Daten, deren Verarbeitung eingeschränkt wurde, von ihrer Speicherung abgesehen nur noch in bestimmten Fällen, zum Beispiel mit Einwilligung der betroffenen Person oder zur Geltendmachung von Rechtsansprüchen, verarbeitet werden.

Da auch eine ganze Vorgangsreihe als Verarbeitung gilt, ist von einem weiten Verarbeitungsbegriff auszugehen. Es wird nicht auf einzelne Phasen eines einheitlichen Vorgangs abgestellt, beispielsweise zur Beantwortung der Frage der datenschutzrechtlichen Zulässigkeit.

2.3. Profiling

Unter Profiling versteht man gemäß Art. 4 Nr. 4 DSGVO jede Art der **automatisierten Verarbeitung** personenbezogener Daten, die darin besteht, diese personenbezogenen Daten zu verwenden, um bestimmte **persönliche Aspekte** in Bezug auf eine natürliche Person zu **bewerten**. Die Bewertung erfolgt hierbei insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit,

[20] Paal/Pauly/Ernst DSGVO Art. 4 Rdnr. 32.
[21] Kühling/Buchner/Herbst DSGVO Art. 4 Nr. 2 Rdnr. 36 f.; Paal/Pauly/Ernst DSGVO Art. 4 Rdnr. 34. S. auch DIN 66399.

persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.
Die Begriffsdefinition des **Profiling** ist insbesondere im Rahmen des Art. 22 DSGVO relevant, in dem **automatisierte Entscheidungen** im Einzelfall einschließlich Profiling geregelt werden. Die betroffene Person hat gemäß Art. 22 Abs. 1 DSGVO das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

2.4. Pseudonymisierung

Gemäß Art. 4 Nr. 5 DSGVO ist unter dem Begriff **Pseudonymisierung** die Verarbeitung personenbezogener Daten in einer Weise zu verstehen, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Laut Erwgr. 26 sollen einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen, zum Beispiel eines Schlüssels bei Verschlüsselung personenbezogener Daten,[22] weiterhin einer natürlichen Person zugeordnet werden könnten, als Informationen über eine identifizierbare natürliche Person betrachtet werden. Daher handelt es sich bei pseudonymisierten Daten um personenbezogene Daten für denjenigen, der die Pseudonymisierung durchgeführt hat und nach der Theorie des relativen Personenbezugs ebenso für Dritte, wenn eine Zuordnung durch diese nach allgemeinem Ermessen wahrscheinlich ist.

Im Gegensatz dazu handelt es sich bei anonymisierten Daten nicht um personenbezogene Daten. Erwgr. 26 führt hierzu aus, dass die Grundsätze des Datenschutzes nicht für anonyme Informationen gelten. Das heißt die Datenschutz-Grundverordnung gilt nicht für Informationen, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Aus Erwgr. 26 wird deutlich, dass die Datenschutz-Grundverordnung – auch wenn sie keine Legaldefinition des Begriffs Anonymität enthält – davon ausgeht, dass Anonymität unwiderruflich ist („nicht oder nicht mehr identifiziert werden kann“).[23]

2.5. Dateisystem

Unter einem Dateisystem ist gemäß Art. 4 Nr. 6 DSGVO jede **strukturierte Sammlung personenbezogener Daten** zu verstehen, die nach **bestimmten Kriterien** zugänglich sind. Für die Begriffsbestimmung des Dateisystems ist es unerheblich, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird. Wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind, soll der Schutz betroffener Personen sowohl bei automatisierter als auch bei manueller Verarbeitung ihrer personenbezogenen Daten bestehen. Nach Erwgr. 25 sollen Akten oder Aktensammlungen sowie ihre Deckblätter in den Anwendungsbereich der

[22] Zur (Un)-Möglichkeit des Entfernens des Personenbezugs mittels Verschlüsselung durch Cloud-Nutzer sowie den diesbzgl. gesetzlichen Regelungsbedarf s. Steidle/Pordesch DuD 2015, 536 (5).
[23] So auch zum bisherigen Recht die (ehemalige) Art. 29-Datenschutzgruppe, WP 216, 5 f.

Datenschutz-Grundverordnung fallen, soweit diese nach bestimmten Kriterien geordnet sind. Auch Video- oder Tonaufnahmen fallen unter den Begriff des Dateisystems, wenn zum Beispiel eine Identifizierung durch Stimmabgleich möglich ist.[24]

2.6. Verantwortlicher und Auftragsverarbeiter

Adressat der Verpflichtungen aus der DSGVO ist in erster Linie der sog. Verantwortliche. Ein für die Verarbeitung personenbezogener Daten Verantwortlicher ist gemäß Art. 4 Nr. 7 DSGVO eine **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. Eine gemeinsame Verantwortung ist beispielsweise zwischen den Betreibern einer **Facebook-Fanpage** und Facebook selbst möglich.[25] Entscheidend bei der Bestimmung des Verantwortlichen ist eine tatsächliche Entscheidungshoheit über Zwecke und Mittel der Datenverarbeitung.[26] Sind die Zwecke und Mittel der Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung gemäß Art. 4 Nr. 7 DSGVO nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

Die (ehemalige) Art. 29-Datenschutzgruppe stellte klar, dass der Begriff des Verantwortlichen primär dazu dienen soll zu bestimmen, wer die Einhaltung der Datenschutz-Grundverordnung und anderer Datenschutzvorschriften zu verantworten hat und durch wen die Rechte der betroffenen Personen sicherzustellen sind. Kurz gesagt dient der Begriff des Verantwortlichen also dazu, die **Verantwortung für die Verarbeitung** personenbezogener Daten zuzuweisen.[27]

Auftragsverarbeiter ist gemäß Art. 4 Nr. 8 DSGVO eine **natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle**, die personenbezogene Daten **im Auftrag des Verantwortlichen** verarbeitet. Das Einschalten eines Auftragsverarbeiters hängt von der Entscheidung des Verantwortlichen ab, personenbezogene Daten nicht innerhalb der eigenen Organisation zu verarbeiten, sondern diese von einem Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeiten zu lassen. Diese Beauftragung erfolgt i.d.R. durch einen Auftragsverarbeitungsvertrag zwischen Verantwortlichem und Auftragsverarbeiter im Sinne des Art. 28 Abs. 3 DSGVO, der unter anderem Gegenstand, Art und Zweck der Verarbeitung festlegt. Art. 29 DSGVO stellt klar, dass der Auftragsverarbeiter entsprechende Daten nur auf Weisung des Verantwortlichen verarbeiten darf. Dies bedeutet, dass der Verantwortliche weiterhin alle wesentlichen Entscheidungen über Zwecke und Mittel der Datenverarbeitung zu treffen hat. Auftragsverarbeiter haben allerdings einen Spielraum, um nicht-wesentliche Entscheidungen bspw. hinsichtlich praktischer Aspekte der Umsetzung der Verarbeitung zu treffen.[28]

Um als Auftragsverarbeiter eingestuft werden zu können, muss eine Organisation in Bezug auf den Verantwortlichen **rechtlich eigenständig** sein.[29] Dabei ist zu beachten, dass eine Organisation regelmäßig nicht ausschließlich die Rolle des Auftragsverarbeiters einnimmt. So kann eine Organisation

[24] Paal/Pauly/Ernst DSGVO Art. 4 Rdnr. 53.
[25] EuGH Urteil vom 5.6.2018 – C-210/16.
[26] Simitis/Hornung/Spiecker/Petri Datenschutzrecht Art. 4 Nr. 7 Rdnr. 20.
[27] (Ehemalige) Art. 29-Datenschutzgruppe, WP 169, 6; sich auf diese Ausführungen beziehend Europäischer Datenschutzausschuss, Leitlinien 07/2020, 9.
[28] Europäischer Datenschutzausschuss, Leitlinien 07/2020, 16 f.; Kühling/Buchner/Hartung DSGVO Art. 4 Nr. 8 Rdnr. 7.
[29] (Ehemalige) Art. 29-Datenschutzgruppe, WP 169, 30.

im Auftrag eines Verantwortlichen personenbezogene Daten von dessen Mitarbeitern und Kunden als Auftragsverarbeiter verarbeiten, ist im Hinblick auf die Verarbeitung der personenbezogenen Daten der eigenen Mitarbeiter jedoch Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Die Zuordnung der Rolle eines Verantwortlichen und Auftragsverarbeiters hat somit immer **für einen konkreten Verarbeitungsvorgang** zu erfolgen.

2.7. Empfänger und Dritter

Ein Empfänger ist gemäß Art. 4 Nr. 9 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten **offengelegt** werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Offengelegt werden personenbezogene Daten, wenn diese anderen Stellen in einer Weise zugänglich werden, dass diese Stellen Kenntnis über den Informationsgehalt der Daten erlangen können.[30]

Nicht als Empfänger gelten gemäß Art. 4 Nr. 9 DSGVO Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten. Die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.

Ein Dritter ist gemäß Art. 4 Nr. 10 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, **außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter** und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten. Bei der Begriffsdefinition des „Dritten" handelt es sich im Wesentlichen um eine Negativabgrenzung zum Begriff der betroffenen Person, dem Verantwortlichen und dem Auftragsverarbeiter. Angewandt wird der Begriff in der DSGVO in erster Linie im Zusammenhang mit der Verwendung der Rechtsgrundlage des berechtigten Interesses des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 lit. f, Art. 13 Abs. 1 lit. d, Art. 14 Abs. 2 lit. b DSGVO).

Grundsätzlich müssen Dritte Personen außerhalb des Verantwortungsbereichs des Verantwortlichen sein und keine von diesem abgeleitete Legitimation zur Verarbeitung der jeweiligen personenbezogenen Daten haben. Damit gelten unselbstständige Unternehmenszweigstellen des Verantwortlichen oder Auftragsverarbeiters beispielsweise nicht als Dritte.[31]

2.8. Einwilligung

Eine Einwilligung ist gemäß Art. 4 Nr. 11 DSGVO jede von der betroffenen Person freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Eine Einwilligung hat regelmäßig vor Beginn der Datenverarbeitung zu erfolgen.

[30] Kühling/Buchner/Herbst DSGVO Art. 4 Nr. 2 Rdnr. 29.
[31] Kühling/Buchner/Hartung DSGVO Art. 4 Nr. 10 Rdnr. 6 f.; Simitis/Hornung/Spiecker/Petri DSGVO Art. 4 Nr. 10 Rdnr. 1.

Die Einwilligung ist eine Rechtsgrundlage nach Art. 6 Abs. 1 lit. a DSGVO zur rechtmäßigen Verarbeitung personenbezogener Daten. Hierbei ist zu beachten, dass es sich bei der Einwilligung nur um eine der möglichen Grundlagen handelt, die zur Rechtmäßigkeit der Verarbeitung führen und daher nicht jede Verarbeitung zwingend eine Einwilligung erfordert.

Eine Einwilligung hat grundsätzlich durch die betroffene Person, einen durch die betroffene Person beauftragten Stellvertreter oder – zum Beispiel im Falle von **Minderjährigen** und **betreuten Personen** – durch den gesetzlichen Vertreter der betroffenen Person zu erfolgen.[32] Eine Entscheidung durch den gesetzlichen Vertreter der betroffenen Person ist jedoch nur dann zulässig, wenn die betroffene Person nicht in der Lage ist, die Einwilligung zu erteilen. Dies wäre zum Beispiel dann der Fall, wenn es der betroffenen Person an der Einsichtsfähigkeit mangelt. Bei der Einwilligung durch einen durch die betroffene Person beauftragten Stellvertreter ist darauf zu achten, dass sich die Vollmacht auf einen konkreten Inhalt bezieht, für den eine Einwilligung erteilt werden soll.[33]

An die Einwilligung eines **Kindes** in Bezug auf Dienste der Informationsgesellschaft stellt Art. 8 DSGVO die besondere Bedingung, dass die Verarbeitung personenbezogener Daten von Kindern, die noch nicht das sechzehnte Lebensjahr vollbracht haben, nur rechtmäßig ist, sofern und soweit die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.[34] Im Zusammenhang mit der Altersverifikation im Internet kann zum Beispiel die Onlineausweisfunktion des Personalausweises verwendet werden.[35]

Eine Einwilligung muss auf Basis der **freiwilligen Entscheidung** einer betroffenen Person erfolgen. Gemeint ist eine echte Wahlmöglichkeit der betroffenen Person hinsichtlich des Ob, Wie, Wieviel und Wem sie die Verarbeitung ihrer personenbezogenen Daten gestattet.[36] Freiwilligkeit liegt spätestens dann nicht mehr vor, wenn die betroffene Person unter Druck gesetzt wird oder (unangemessene) Nachteile zu befürchten hätte, wenn sie die Einwilligung nicht erteilen würde.

Eine Einwilligung muss für einen **bestimmten Fall** erfolgen. Ausgeschlossen sind somit Einwilligungserklärungen, die einem oder mehreren Verantwortlichen die Verarbeitung personenbezogener Daten auf pauschale Weise erlauben sollen. Vielmehr hat die Einwilligung den Zweck, Umfang und Verantwortlichen konkret zu bestimmen.

Die Abgabe einer Einwilligung in informierter Weise setzt voraus, dass die betroffene Person die Möglichkeit hatte, von dem **Inhalt der Einwilligungserklärung in zumutbarer Weise Kenntnis zu erlangen**. Dies ist zum Beispiel bei vorformulierten Einwilligungserklärungen und Datenschutzhinweisen

[32] S. hierzu auch Paal/Pauly/Ernst DSGVO Art. 4 Rdnr. 63 ff., der diese Ansicht für Minderjährige vertritt und für betreute Personen nahelegt.
[33] Gola/Heckmann/Gola DSGVO Art. 4 Rdnr. 105.
[34] Die Mitgliedstaaten können durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf, s. Art. 8 Abs. 1 S. 3 DSGVO.
[35] Die Altersverifikation kann hierbei über die Onlineausweisfunktion des Personalausweises so datensparsam gestaltet werden, dass der Verantwortliche lediglich die Information „über 16 Jahre alt", ohne Angabe des Geburtsdatums, erhält. BSI Technische Richtlinie TR-03127, 23 f. Gleichwohl wird international agierenden Unternehmen eine rein deutsche Lösung zur Altersverifikation nicht ausreichen, jedoch gibt es auch in anderen EU-Mitgliedstaaten entsprechende nationale eID-Lösungen, die die Altersverifikation ermöglichen. Durch die VO über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO, 910/2014) ist es möglich, die nationalen Lösungen innerhalb der EU-Länder-übergreifend einzusetzen.
[36] Paal/Pauly/Ernst DSGVO Art. 4 Rdnr. 69.

der Fall. Dagegen kann unter anderem bei versteckten Hinweisen, überlangen Texten und Sprachbarrieren nicht von einer in informierter Weise abgegebenen Einwilligung ausgegangen werden.[37] Wird die betroffene Person auf elektronischem Weg zur Einwilligung aufgefordert, so muss die Aufforderung laut Erwgr. 32 in **klarer und knapper Form** und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgen. Zu berücksichtigen gilt es hierbei jedoch, dass dies so ausgestaltet werden muss, dass kein Widerspruch zu den Informationspflichten nach Art. 13, 14 DSGVO entsteht. Die Einwilligung soll durch eine **eindeutige bestätigende Handlung** erfolgen. Dies kann etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung erfolgen. Das **Anklicken eines Kästchens beim Besuch einer Internetseite**, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert, ist ausdrücklich möglich. Dagegen erfüllen Stillschweigen, bereits angekreuzten Kästchen – auch im Zusammenhang mit dem Besuch einer Internetseite – oder Untätigkeit der betroffenen Person laut Erwgr. 32 nicht die Anforderung an eine eindeutige bestätigende Handlung.

Sollen **besondere Kategorien** personenbezogener Daten verarbeitet werden, so ist die betroffene Person gemäß Art. 9 Abs. 2 lit. a DSGVO regelmäßig ausdrücklich auf die Verarbeitung dieser Daten **hinzuweisen**. Diese zusätzliche Voraussetzung der Ausdrücklichkeit der Einwilligung im Zusammenhang mit der Verarbeitung besonderer Kategorien personenbezogener Daten bezieht sich darauf, wie eine betroffene Person ihre Einwilligung zum Ausdruck bringt und erfordert regelmäßig zusätzliche Anstrengungen des Verantwortlichen, um die sicherzustellen.[38]

2.9. Verletzung des Schutzes personenbezogener Daten

Eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, wird gemäß Art. 4 Nr. 12 DSGVO als Verletzung des Schutzes personenbezogener Daten bezeichnet. Laut der Legaldefinition ist es unerheblich, ob die Verletzung unbeabsichtigt oder unrechtmäßig erfolgte. Die Bezeichnung als „Verletzung des Schutzes personenbezogener Daten" scheint etwas unglücklich gewählt, stellt die Definition doch sogleich klar, dass es sich um eine „Verletzung der Sicherheit" handelt. Eindeutiger ist in diesem Sinne die englische Begriffsbestimmung „personal data breach", die den Sicherheitsaspekt bereits im Namen stärker fokussiert.

Die Definition hat insbesondere in Bezug auf Art. 33 und 34 DSGVO Relevanz. Art. 33 DSGVO regelt die **Meldung** von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, die unverzüglich zu erfolgen hat, wobei Absatz 1 konkretisiert, dass die Meldung möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, erfolgen soll und der Meldung eine Begründung für die Verzögerung beizufügen ist, wenn diese nicht binnen 72 Stunden erfolgt. Art. 34 regelt die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die

[37] Paal/Pauly/Ernst DSGVO Art. 4 Rdnr. 79 bis 84.
[38] Europäischer Datenschutzausschuss, Leitlinien 05/2020, S. 24.

persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. Auch diese Meldung hat unverzüglich zu erfolgen.[39]

2.10. Genetische, biometrische Daten und Gesundheitsdaten

Art. 9 Abs. 1 DSGVO untersagt die Verarbeitung **besonderer Kategorien personenbezogener Daten**, zu denen diejenigen Daten zählen, aus denen zum Beispiel die rassische[40] und ethnische Herkunft, politische Meinungen, religiöse, weltanschauliche Überzeugungen hervorgehen, sowie Daten zum Sexualleben und der sexuellen Orientierung einer natürlichen Person. Zu den besonderen Kategorien personenbezogener Daten, deren Verarbeitung durch Art. 9 DSGVO beschränkt wird, zählen auch genetische Daten. Nach Art. 4 Nr. 13 DSGVO sind genetische Daten personenbezogene Daten zu den **ererbten oder erworbenen genetischen Eigenschaften** einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden. Erwgr. 34 konkretisiert diese Definition im Hinblick darauf, dass die ererbten oder erworbenen genetischen Eigenschaften aus der Analyse einer biologischen Probe der betreffenden natürlichen Person, insbesondere durch eine Chromosomen, Desoxyribonukleinsäure (DNS)- oder Ribonukleinsäure (RNS)-Analyse oder der Analyse eines anderen Elements, durch die gleichwertige Informationen erlangt werden können, gewonnen werden.
Besonders zu berücksichtigen ist im Hinblick auf genetische Daten zum einen der Umstand, dass die Interessen der betroffenen Person mit den Interessen seiner **Verwandten** (oder noch ungeborenen Kinder) kollidieren können, zu denen aus den genetischen Daten der betroffenen Person Rückschlüsse gezogen werden können. So können aus genetischen Daten wesentliche Vorhersagen zum Gesundheitszustand einer betroffenen Person gemacht werden was zum Beispiel Versicherungen bei der Tarifierung berücksichtigen können.[41]

Biometrische Daten gehören ebenfalls zu den besonderen Kategorien personenbezogener Daten[42] und sind gemäß Art. 4 Nr. 14 DSGVO mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den **physischen, physiologischen oder verhaltenstypischen Merkmalen** einer natürlichen Person, die die **eindeutige Identifizierung** dieser natürlichen Person ermöglichen oder bestätigen. Beispiele für biometrische Daten sind Fingerabdrücke und Gesichtsbilder in Form eines biometrischen Lichtbildes. Die Verarbeitung von Lichtbildern sollte jedoch laut Erwgr. 51 nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden, da Lichtbilder nur dann von der Definition des Begriffs biometrische Daten erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen. Eine eindeutige Identifizierbarkeit dürfte mit modernen Digitalkameras zunehmend der Regelfall werden.

[39] Für Ausnahmen von der Benachrichtigungspflicht s. Art. 34 Abs. 3 DSGVO.
[40] In Erwgr. 51 DSGVO wird hierzu klargestellt, dass die Verwendung des Begriffs „rassische Herkunft" in der DSGVO nicht bedeutet, dass die europäische Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt.
[41] Paal/Pauly/Ernst DSGVO Art. 4 Rdnr. 96.
[42] Für das Verarbeitungsverbot und seine Ausnahmen vgl. Art. 9 DSGVO.

Es ist davon auszugehen, dass die Bedeutung biometrischer Daten in Zukunft immer weiter zunehmen wird. So können zum Beispiel bei der Nutzung von Webseiten über den Computer und/oder das Smartphone mithilfe technologischer Entwicklungen sogenannte „**behavioural biometrics**" erhoben werden, die unter anderem das Eingabeverhalten, typische Handbewegungen, Tipprhythmus und die Reaktionszeit von Webseitennutzern analysieren und zu einem Profil kombinieren können. Die Profile, die durch die Analyse dieser Daten entstehen, sind mit sehr hoher Wahrscheinlichkeit einzigartig.[43] Es ist somit analog Erwgr. 51 davon auszugehen, dass diese Daten dann als biometrische Daten anzusehen sind, wenn diese mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen.

Auch **Gesundheitsdaten** stellen eine besondere Kategorie personenbezogener Daten dar[44] und sind gemäß Art. 4 Nr. 15 DSGVO personenbezogene Daten, die sich auf die **körperliche oder geistige Gesundheit** einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Die Informationen können sich sowohl auf den früheren und gegenwärtigen als auch auf den künftigen Gesundheitszustand beziehen. Der Begriff der Gesundheitsdaten ist weit auszulegen, so dass laut Erwgr. 35 nicht nur Informationen, die sich aus biologischen Proben ableiten lassen, sowie Informationen über Krankheiten, klinische Behandlungen und Krankheitsrisiken, sondern unter anderem auch Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren unter den Begriff fallen sollen. Dies ist unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-Vitro-Diagnostikum stammen.

Aufgrund der bewusst weit gewählten Auslegung des Begriffs der Gesundheitsdaten in Erwgr. 35 ist davon auszugehen, dass auch die im Abschnitt zu „biometrischen Daten" diskutierten „**behavioural biometrics**" im Rahmen der Begriffsdefinition der Gesundheitsdaten Relevanz entfalten können. Dies ist insbesondere dann der Fall, wenn sie einer Person mit sehr hoher Wahrscheinlichkeit eindeutig zugeordnet werden können und durch deren Analyse unter Umständen Rückschlüsse zum Gesundheitszustand der betroffenen Person möglich werden. Auch im Zusammenhang mit **Gesundheits- oder Fitness-Apps** kann der Begriff der Gesundheitsdaten einschlägig sein, da bei Gesundheits-Apps Analysen erfolgen können, die Rückschlüsse auf sensible Eigenschaften zum Gesundheitszustand einer betroffenen Person ermöglichen.

2.11. Hauptniederlassung, Vertreter und Unternehmen

Eine **Niederlassung** setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung ist dabei laut Erwgr. 22 nicht ausschlaggebend.

Im Falle eines Verantwortlichen mit **Niederlassungen in mehr als einem Mitgliedstaat** ist die **Hauptniederlassung** gemäß Art. 4 Nr. 16 lit. a DSGVO der Ort seiner Hauptverwaltung in der Union.

[43] Turgeman/Zelazny 2017, 5 (5 bis 7).
[44] Für das Verarbeitungsverbot und seine Ausnahmen vgl. Art. 9 DSGVO.

Dies gilt nicht, wenn die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten in einer anderen Niederlassung des Verantwortlichen in der Union getroffen werden und diese Niederlassung befugt ist, diese Entscheidungen umsetzen zu lassen. In diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung. Zur Bestimmung der Hauptniederlassung eines Verantwortlichen in der Union sollten **objektive Kriterien** herangezogen werden, wie zum Beispiel die effektive und tatsächliche Ausübung von Managementtätigkeiten durch eine feste Einrichtung, in deren Rahmen die Grundsatzentscheidungen zur Festlegung der Zwecke und Mittel der Verarbeitung getroffen werde. Dabei sollte nicht ausschlaggebend sein, ob die Verarbeitung der personenbezogenen Daten tatsächlich an diesem Ort ausgeführt wird.[45]

Im Falle eines **Auftragsverarbeiters** mit Niederlassungen in mehr als einem Mitgliedstaat ist die Hauptniederlassung gemäß Art. 4 Nr. 16 lit. b DSGVO ebenfalls der Ort seiner Hauptverwaltung in der Union oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt.

Im Falle einer **Unternehmensgruppe** sollte laut Erwgr. 36 die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten, es sei denn, die Zwecke und Mittel der Verarbeitung werden von einem anderen Unternehmen festgelegt.

Gemäß Art. 3 Abs. 2 DSGVO erstreckt sich der territoriale Anwendungsbereich der Datenschutz-Grundverordnung nach dem sogenannten **Marktortprinzip** auch auf Verantwortliche und Auftragsverarbeiter, die **keine Niederlassung** in der Union haben, wenn die Datenverarbeitung im Zusammenhang damit steht, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten oder das Verhalten betroffener Personen zu beobachten. Teilweise leugneten Globalplayer im Internet, dass sie europäisches Datenschutzrecht beachten müssen und der Kontrolle der europäischen Aufsichtsbehörden unterliegen. Die Datenschutz-Grundverordnung stellt klar, dass ein Verantwortlicher oder Auftragsverarbeiter im Drittstaat unter den genannten Voraussetzungen dem europäischen Datenschutzrecht und der Kontrolle der europäischen Aufsichtsbehörden unterliegt. Ohne einen Vertreter in der Union wäre der Verantwortliche oder der Auftragsverarbeiter jedoch nicht unmittelbar für die Aufsichtsbehörden greifbar und auch die betroffenen Personen müssten zur Ausübung der Betroffenenrechte eine Stelle in einem Drittstaat kontaktieren. Dementsprechend hat der Verantwortliche oder der Auftragsverarbeiter im Drittstaat einen Vertreter zu benennen.[46]

Bei einem **Vertreter** handelt es sich gemäß Art. 4 Nr. 17 DSGVO um eine **in der Union niedergelassene** natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Art. 27 DSGVO[47] bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt. Zu beachten gilt, dass es nicht irrelevant ist, wo in der Union der Vertreter niedergelassen ist. Art. 27 Abs. 3 DSGVO konkretisiert diesbezüglich, dass der Vertreter in einem der Mitgliedstaaten niedergelassen sein

[45] Erwgr. 36. Das Vorhandensein und die Verwendung technischer Mittel und Verfahren zur Verarbeitung personenbezogener Daten oder Verarbeitungstätigkeiten begründen an sich noch keine Hauptniederlassung und sind daher laut Erwgr. 36 kein ausschlaggebender Faktor für das Bestehen einer Hauptniederlassung.
[46] Gola/Heckmann/Gola DSGVO Art. 4 Rdnr. 131.
[47] Art. 27 DSGVO regelt die Vertretung von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern.

muss, in denen die betroffenen Personen, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird, sich befinden. Die Funktion des Vertreters kann zum Beispiel einem freien Mitarbeiter, einem Rechtsanwalt oder einer juristischen Person übertragen werden.[48]

Bei einem Unternehmen handelt es sich gemäß Art. 4 Nr. 18 DSGVO um eine **natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt**. Dies ist unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen.

Der **Unternehmensbegriff** der Datenschutz-Grundverordnung ist sehr weit gefasst – unerheblich sind unter anderem die Branche und Größe eines Unternehmens, so dass auch **Freiberufler und Kleinstunternehmen** unter den Begriff fallen. Zieht eine Person aus einer Tätigkeit sowohl privaten als auch beruflichen Nutzen (**Dual Use**), ist der Unternehmensbegriff erfüllt.[49]

Bei einer **Unternehmensgruppe** handelt es sich gemäß Art. 4 Nr. 19 DSGVO um eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht. Hintergrund dieser Definition ist das Verständnis, dass ein Unternehmen, das die Verarbeitung personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert, mit diesen zusammen als eine Unternehmensgruppe betrachtet werden sollte. Das herrschende Unternehmen sollte laut Erwgr. 37 dasjenige Unternehmen sein, das zum Beispiel aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen **beherrschenden Einfluss** auf die übrigen Unternehmen ausüben kann.

Der Begriff hat unter anderem Bedeutung für die Benennung eines **gemeinsamen Datenschutzbeauftragten** gemäß Art. 37 DSGVO und für die Aufstellung **verbindlicher interner Datenschutzvorschriften** gemäß Art. 47 DSGVO.

2.12. Verbindliche interne Datenschutzvorschriften

Verbindliche interne Datenschutzvorschriften sind gemäß Art. 4 Nr. 20 DSGVO Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter – im Hinblick auf Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern – **selbst verpflichtet**. Die Anwendung verbindlicher interner Datenschutzvorschriften auch als sogenannte **Binding Corporate Rules** bezeichnet, wird in Art. 47 DSGVO geregelt.

[48] Gola/Heckmann/Gola DSGVO Art. 4 Rdnr. 131.
[49] Paal/Pauly/Ernst DSGVO Art. 4 Rdnr. 124 f.; Taeger/Gabel/Arning/Rothkegel DSGVO Art. 4 Rdnr. 442 bis 444.

2.13. (Betroffene) Aufsichtsbehörde

Laut der Legaldefinition des Art. 4 Nr. 21 DSGVO ist eine **Aufsichtsbehörde** eine von einem Mitgliedstaat gemäß Art. 51 eingerichtete **unabhängige staatliche Stelle**, welche für die **Überwachung** der Anwendung der Datenschutz-Grundverordnung zuständig ist, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird.[50] Den Mitgliedsstaaten steht es frei, eine oder – wie in Deutschland durch den Bundes- und die Landesbeauftragten für Datenschutz und Informationsfreiheit – mehrere unabhängige Behörden mit dieser Aufgabe zu betrauen.

Eine betroffene Aufsichtsbehörde ist gemäß Art. 4 Nr. 22 DSGVO eine Aufsichtsbehörde, die **von der Verarbeitung** personenbezogener Daten **betroffen** ist, weil der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist oder diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde. Demnach können im Rahmen eines Verfahrens mehrere Aufsichtsbehörden als betroffene Aufsichtsbehörden gelten. Die betroffenen Aufsichtsbehörden arbeiten unter der Leitung der sog. federführenden Aufsichtsbehörde bei grenzüberschreitenden Verarbeitungen nach Art. 56 Abs. 1, Art. 60 DSGVO zusammen.

2.14. Grenzüberschreitende Verarbeitung

Bei der grenzüberschreitenden Verarbeitung unterscheidet die Legaldefinition nach Art. 4 Nr. 23 lit. a und lit. b DSGVO zwei Fälle: Eine grenzüberschreitende Verarbeitung liegt einerseits vor, wenn eine Verarbeitung personenbezogener Daten **im Rahmen der Tätigkeiten von mehreren Niederlassungen** eines Verantwortlichen beziehungsweise Auftragsverarbeiters in der Union **in mehr als einem Mitgliedstaat** erfolgt und der Verantwortliche beziehungsweise Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist (lit. a). Andererseits liegt eine grenzüberschreitende Verarbeitung vor, wenn eine Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten **einer einzelnen Niederlassung** eines Verantwortlichen oder Auftragsverarbeiters in der Union erfolgt, die **erhebliche Auswirkungen** auf betroffene Personen in mehr als einem Mitgliedstaat haben kann (lit. b). Damit erfasst der Begriff Vorgänge, die grenzüberschreitend mehrere Staaten innerhalb der EU betreffen. In Abgrenzung zu Datenübermittlungen, die an Länder außerhalb der EU stattfinden, wird hierfür der Begriff „Drittländer" verwendet.[51] Die Legaldefinition entfaltet seine Relevanz bei der Bestimmung der federführenden Aufsichtsbehörde im Sinne des Art. 56 DSGVO. Im Falle der grenzüberschreitenden Verarbeitung soll die Aufsichtsbehörde für die Hauptniederlassung des Verantwortlichen oder Auftragsverarbeiters oder für die einzige Niederlassung des Verantwortlichen oder Auftragsverarbeiters als federführende Behörde fungieren und mit anderen Behörden zusammenarbeiten, wenn zum Beispiel die Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz in deren Hoheitsgebiet hat oder weil bei diesen eine Beschwerde eingelegt wurde.[52]

[50] S. hierzu auch Art. 51 Abs. 1 DSGVO.
[51] S. hierzu auch Art. 44 ff. DSGVO.
[52] S. hierzu auch Erwgr. 124.

2.15. Maßgeblicher und begründeter Einspruch

Die Definition des maßgeblichen und begründeten Einspruchs entfaltet ihre Relevanz im Hinblick auf die **Zusammenarbeit mehrerer betroffener Aufsichtsbehörden nach Art. 60 DSGVO**. Die federführende Aufsichtsbehörde hat den anderen betroffenen Aufsichtsbehörden im Rahmen dieser Zusammenarbeit – zum Beispiel bezüglich einer Maßnahme in Folge eines Datenschutzverstoßes – einen Beschlussentwurf zur Stellungnahme vorzulegen und trägt deren Standpunkten gebührend Rechnung. Legt eine der anderen betroffenen Aufsichtsbehörden gegen diesen Beschlussentwurf einen maßgeblichen und begründeten Einspruch ein und schließt sich die federführende Aufsichtsbehörde dem maßgeblichen und begründeten Einspruch nicht an oder ist der Ansicht, dass der Einspruch nicht maßgeblich oder nicht begründet ist, so leitet die federführende Aufsichtsbehörde das Kohärenzverfahren gemäß Art. 63 DSGVO ein.

Gemäß Art. 4 Nr. 24 DSGVO ist ein **maßgeblicher und begründeter Einspruch** ein Einspruch im Hinblick darauf, ob ein Verstoß gegen diese Verordnung vorliegt oder nicht oder ob die beabsichtigte Maßnahme gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung steht, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen. Insofern gibt die Definition des maßgeblichen und begründeten Einspruchs die formalen Voraussetzungen an einen Einspruch gegen einen Beschlussentwurf wieder.[53]

2.16. Dienst der Informationsgesellschaft

Für die Definition des **Dienstes der Informationsgesellschaft** verweist Art. 4 Nr. 25 DSGVO auf die Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates. Laut Art. 1 Abs. 1 lit. b der Richtlinie ist unter einer Dienstleistung der Informationsgesellschaft jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung zu verstehen. Die Definition unterscheidet im Fernabsatz, elektronisch und auf individuellen Abruf eines Empfängers erbrachte Dienstleistungen.

Unter den Begriff des Dienstes der Informationsgesellschaft fallen gemäß Art. 1 Abs. 1 lit. b i) sowie Anhang 1 Nr. 1 der Info-Richtlinie[54] zunächst **im Fernabsatz erbrachte Dienstleistungen**. Hierbei handelt es sich um Dienstleistungen, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht wird. Bei Diensten, bei deren Erbringung der Erbringer und der Empfänger **gleichzeitig physisch** anwesend sind, handelt es sich hingegen **nicht um Dienste der Informationsgesellschaft**, selbst wenn dabei elektronische Geräte benutzt werden. Somit sind unter anderem die Konsultation eines elektronischen Katalogs in einem Geschäft in Anwesenheit des Kunden und die Buchung eines Flugtickets über ein Computernetz, wenn sie in einem Reisebüro in Anwesenheit des Kunden vorgenommen wird nicht von der Begriffsdefinition des Dienstes der Informationsgesellschaft umfasst.
Unter den Begriff des Dienstes der Informationsgesellschaft fallen nach Art. 1 Abs. 1 lit. b ii) sowie Anhang 1 Nr. 2 Info-RL auch elektronisch erbrachte Dienstleistung, so zum Beispiel Dienstleistungen, die

[53] Paal/Pauly/Ernst DSGVO Art. 4 Rdnr. 141.
[54] Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9.9.2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft.

mittels Geräten für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen werden und die **vollständig** über Draht, über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen werden. Nicht elektronisch erbrachte Dienste, wie zum Beispiel die Geldausgabe über Geldautomaten sowie der Offline-Vertrieb von Software fallen gemäß Art. 1 Abs. 1 lit. b ii) sowie Anhang 1 Nr. 2 Info-RL nicht unter die Begriffsdefinition.

Darüber hinaus fallen unter den Begriff des Dienstes der Informationsgesellschaft gemäß Art. 1 Abs. 1 lit. b iii) sowie Anhang 1 Nr. 3 Info-RL auf individuellen Abruf eines Empfängers erbrachte Dienstleistungen, also Dienstleistungen, die durch die Übertragung von Daten auf **individuelle Anforderung** erbracht werden. Demgegenüber sind diejenigen Dienste nicht von der Definition des Dienstes der Informationsgesellschaft umfasst, die im Wege einer Übertragung von Daten ohne individuellen Abruf gleichzeitig für eine unbegrenzte Zahl von einzelnen Empfängern erbracht werden, wie zum Beispiel Fernseh- und Hörfunkdienste.

Im Rahmen der DSGVO wird der Begriff der Dienste der Informationsgesellschaft beispielsweise im Zusammenhang mit den Bedingungen einer Einwilligung bei Kindern nach Art. 8 DSGVO verwendet.

2.17. Internationale Organisation

Unter einer **internationalen Organisation** sind gemäß Art. 4 Nr. 26 DSGVO **völkerrechtliche Organisationen und ihre nachgeordneten Stellen** oder jede sonstige Einrichtung zu verstehen, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde. Unter den Begriff fallen unter anderem die Vereinten Nationen, die Welthandelsorganisation und die Europäische Union. Nicht-staatliche internationale Organisationen, wie zum Beispiel Greenpeace, fallen hingegen nicht unter den Begriff.[55]

[55] Taeger/Gabel/Arning/Rothkegel DSGVO Art. 4 Rdnr. 509.

Literaturverzeichnis

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

Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03127, Version 1.21, 2. Mai 2018, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03127/BSI-TR-03127.pdf?__blob=publicationFile&v=2.

Europäischer Datenschutzausschuss, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2026/679, Version 1.1, angenommen am 4. Mai 2020, abrufbar unter: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf.

Europäischer Datenschutzausschuss, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0, angenommen am 7. Juli 2021, abrufbar unter: https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_de.pdf.

Finck, M./Pallas, F., They who must not be identified—distinguishing personal from non-personal data under the GDPR, International Data Privacy Law 2020, 10(1), 11-36.

Gola, P./Heckmann, D. (Hrsg.), Datenschutz-Grundverordnung - Bundesdatenschutzgesetz (Kommentar), 3. Aufl., München 2022.

Hofmann, J./Johannes, P., DS-GVO: Anleitung zur autonomen Auslegung des Personenbezugs, in: Zeitschrift für Datenschutz, ZD 2017, 221.

Kühling, J./Buchner, B. (Hrsg.), Datenschutz-Grundverordnung/BDSG (Kommentar), 4. Aufl., München 2024.

Paal, B. P. /Pauly, D. A. (Hrsg.), Beck´scher Kompakt-Kommentar Datenschutz-Grundverordnung, 3. Aufl., München 2021.

Selzer, A. (Hrsg.), Datenschutzrecht- Ein Kommentar für Studium und Praxis, 1. Aufl., Stuttgart 2022.

Simitis, S./Hornung, G./Spiecker gen. Döhmann, I. (Hrsg.), Datenschutzrecht – DSGVO mit BDSG, 1. Aufl., Baden-Baden 2019.

Steidle, R./Pordesch, U., Im Netz von Google – Web-Tracking und Datenschutz, DuD 2008, 324.

Turgeman, A./Zelazny, F., Invisible challenges: the next step in behavioural biometrics?, Biometric Technology Today 06/2017, 5.

Taeger, J./Gabel, D. (Hrsg.), DSGVO – BDSG – TTDSG, 4. Aufl., Frankfurt 2022.

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit