II. Begriffe der DSGVO

In jedem Rechtsgebiet gibt es wichtige Begriffe, das ist im Datenschutzrecht und auch im konkreten Fall der DSGVO nicht anders. Die Begriffe sind etwas anders als im BDSG und auch eigenständig, also vor dem Hintergrund der DSGVO, auszulegen. **Was ähnlich heißt, muss nicht dasselbe sein.** Die wichtigste Definitionsnorm der DSGVO ist Art. 4. Insgesamt gibt es in der DSGVO 26 legaldefinierte Begriffe. Die wichtigsten sind:

1. „Personenbezogene Daten"

Die „personenbezogenen Daten" sind in der DSGVO neu definiert, dieser Begriff ist weiter als der bisher im deutschen Datenschutzrecht verwendete. **Personenbezogene Daten** sind ausweislich Art. 4 Nr. 1 DSGVO **alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen**; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Das gilt – und dies ist insbesondere für die Anwaltswebsite interessant – auch für im Internet zugängliche Daten, die einer Online-Kennung zuordnungsfähig sind und die man nicht immer auf den ersten Blick als personenbezogene Daten erkennt, wie z. B. **IP-Adressen und Cookie-Kennungen** (Erwägungsgrund 30 DSGVO). IP-Adressen waren auch bereits nach BDSG-alt personenbezogene Daten (BGH, Urteil vom 15. Mai 2017 – VI ZR 135/13).

Immer dann, wenn man die Daten also einem Menschen zuordnen kann – auch wenn dies nur indirekt aufgrund verschiedener Identifizierungsmerkmale möglich ist – liegen personenbezogene Daten vor.

Das bedeutet auch: **Es gilt ein absoluter Personenbezugsbegriff**. Es ist egal, ob ich bzw. ein Mitarbeiter meiner Kanzlei einen Personenbezug herstellen kann oder ob dies ein Dritter kann – wichtig ist nur, ob dieser Bezug objektiv herstellbar ist.

In Erwägungsgrund 26 gibt es hier weitere Informationen: „*Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Wissen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren*".

Für **anonymisierte Daten** gelten die Grundsätze des Datenschutzes nicht: Diese beziehen sich schließlich nicht auf einen identifizierten oder identifizierbaren Menschen (Erwägungsgrund 26 Satz 5 und 6 DSGVO). Bei der Verarbeitung von **pseudonymisierten Daten** gilt: Diese ist gemäß Art. 4 Nr. 5 DSGVO definiert als *die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.* Also: Statt Namen gibt es ein Pseudonym, und das soll auch nicht wieder aufgelöst werden. Pseudonymisierte Daten sind selbstverständlich aus Sicht des Datenschutzes, wann immer dies umsetzbar ist, personenbezogenen Daten vorzuziehen, da hier die Risiken für die Betroffenen deutlich geringer sind. Deshalb lässt es die DSGVO auch zu, dass Pseudonymisierung bei einem Verantwortlichen für einen bestimmten Zweck dadurch möglich ist, dass zwar theoretisch eine Auflösung der Pseudonymisierung möglich ist, aber Daten durch geeignete Maßnahmen getrennt werden (Erwägungsgrund 29). Die Daten sind also z. B. getrennt gespeichert und es ist durch verbindliche organisatorische Regeln sichergestellt, dass sie nicht genutzt werden, um ein Pseudonym zu identifizieren. Dennoch bleiben es personenbezogene Daten, wenn das Pyseudonym durch irgendjemanden auflösbar ist.

Besonders für Kollegen, die im Erbrecht tätig sind, interessant: **Daten Verstorbener sind keine personenbezogenen Daten im Sinne der DSGVO**. Das ist zwar in der Legaldefinition nicht erwähnt, ergibt sich jedoch aus Erwägungsgrund 27. Das schließt aber nicht aus, dass es anderweitige Rechtsnormen zum Persönlichkeitsschutz auch über den Tod hinaus gibt.

Die DSGVO schützt nur natürliche Personen, also Menschen. **Unternehmensdaten sind nicht umfasst** (Erwägungsgrund 14). In einigen EU-Staaten war (und ist) dies anders: dort gibt es auch ein Unternehmenspersönlichkeitsrecht und auch einen Datenschutz für Unternehmensdaten. Die DSGVO lässt zu, dass dies auch in Zukunft so ist. In Deutschland war und ist die Rechtslage jedoch so, dass die Beschränkung auf natürliche Personen gilt.

2. „Betroffene Person“

Dieser Begriff ersetzt den bisherigen Begriff des „Betroffenen“. Es handelt sich um die identifizierbare oder identifizierte natürliche Person (Art. 4 Nr. 1 DSGVO), auf die sich die Daten beziehen.

3. „Besondere Kategorien personenbezogener Daten“ gemäß Art. 9 DSGVO

In Art. 9 DSGVO sind „besondere Kategorien personenbezogener Daten“ definiert. Dies sind personenbezogene Daten, die ihrem Wesen nach **hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel** sind, weil aus ihnen Folgendes hervorgeht:
– rassische und ethnische Herkunft,
– politische Meinungen,
– religiöse oder weltanschauliche Überzeugungen,
– Gewerkschaftszugehörigkeit.

Erfasst ist auch die Verarbeitung von
– genetischen Daten,
– biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
– Gesundheitsdaten,
– Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Auch die besonderen Kategorien personenbezogener Daten kommen einem im Datenschutzrecht tätigen Anwalt bekannt vor – dies gab es bereits in § 3 Abs. 9 BDSG. Viel hat sich an dieser Stelle nicht geändert: Die Definition ist lediglich um genetische Angaben sowie biometrische Daten zur eindeutigen Identifizierung einer Person ergänzt worden. Während Fingerabdrücke, bspw. als Erkennungsmerkmal, oder Iriserkennung sicher sowohl technisch als auch datenschutzrechtlich eine spannende Aufgabe und Thematik sind, dürften derartige Daten in der Rechtsanwaltskanzlei eher selten vorkommen.

Sind auch **Fotos**, etwa von Mitarbeiterinnen und Mitarbeitern (für die Homepage z. B.) derartige besonders sensible Daten? Nicht immer. Erwägungsgrund 51 meint dazu: „*Die Verarbeitung von Lichtbildern sollte nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden, da Lichtbilder nur dann von der Definition des Begriffs ‚biometrische Daten‘ erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen.*“

Wofür ist die Einordnung von Daten als besondere Kategorie wichtig? Für die Anforderungen an die Rechtmäßigkeit der Datennutzung.

Für diese Datenkategorie gilt ein besonderer Schutz. Das bedeutet: Grundsätzliches Verbot der Verarbeitung mit nur wenigen Ausnahmen. Wann derartige Daten genutzt werden dürfen, ist in Art. 9 Abs. 2 a bis j DSGVO festgelegt. Da ist natürlich der Fall der **Einwilligung**, aber es gibt auch **einige gesetzliche Rechtfertigungsmöglichkeiten**. Bei der Einwilligung ist jedoch besonders zu beachten, dass die Angelegenheit aufgrund der hohen Schutz-

bedürftigkeit der Daten kritisch ist. Auch muss gemäß Erwägungsgrund 51 die Verarbeitung dieser Daten in der Einwilligungserklärung ausdrücklich vorgesehen werden, darüber hinaus gelten auch die weiteren Voraussetzungen einer wirksamen Einwilligung (s. dazu Abschnitte II. 6 und V. 1 a). Es ist damit zu rechnen, dass deshalb der europäische oder deutsche Gesetzgeber tätig wird und weitere Voraussetzungen definiert, wann eingewilligt werden darf.

Auch für die **automatisierte Entscheidungsfindung** gibt es bei dieser Datenkategorie strenge Einschränkungen (Art. 22 Abs. 4 DSGVO). Eine ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhende Entscheidung, die einer Person gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, darf nur unter ganz strengen Voraussetzungen auf den besonderen Kategorien personenbezogener Daten beruhen. Werden derartig schutzbedürftige Daten in hohem Umfang verarbeitet, muss immer, egal wie groß das Unternehmen ist, ein Datenschutzbeauftragter bestellt werden (Art. 37 Abs. 1 c DSGVO), und eine Datenschutz-Folgenabschätzung (dazu Abschnitt IX. 1) ist fällig (Art. 35 Abs. 3 DSGVO). Auch muss dann ein **Verzeichnis der Verarbeitungstätigkeiten** geführt werden.

Als **Berufsgeheimnisträger** dürfen Anwälte gemäß Art. 9 Abs. 2 h in Verbindung mit Abs. 3 besondere Datenkategorien verarbeiten. Dennoch ist darauf zu achten, dass die Datenkategorien im Verarbeitungsverzeichnis gesondert ausgewiesen sind und dass diese Datenkategorien auch im Notfallplan und Maßnahmenkatalog zur Datensicherung gesondert ausgewiesen und besonderen Maßnahmen bedacht werden. Für die Kanzlei wesentlich ist hier insbesondere das Thema Gesundheitsdaten. Es kann aber auch durchaus sein, dass andere derartige Daten im Zusammenhang mit Mandaten bekannt werden oder sogar in Rechtsstreitigkeiten eine zentrale Rolle spielen. Dann ist wichtig, dass hier stets die „rote Lampe“ angeht. Bitte denken Sie auch daran, den „Check“ auf besondere Arten personenbedingt bezogener Daten in die Abläufe aufzunehmen, damit diese Daten sofort erkannt und entsprechend geschützt werden können.

Die Mitgliedsstaaten dürfen außerdem noch weitere Bedingungen definieren, was die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten angeht. Es bleibt also zu beobachten, wie sich die datenschutzrechtliche Rechtslage hinsichtlich dieser besonders geschützten Daten entwickelt. Wichtig ist insbesondere die Datenschutz-Folgenabschätzung. In einer Information des Bayerischen Landesamts für die Datenschutzaufsicht klingt an, dass die Datenschutzaufsichtsbehörden „Interesse daran haben, frühzeitig abgestimmte Informationen für Verantwortliche bereit zu halten“. Hier gilt es also auch, die entsprechenden Internetseiten und Informationsdienste zu beobachten. **Wird hierzu etwas veröffentlicht, werde ich es auch auf der Webseite zu diesem Buch bekanntgeben.**

4. „Verantwortlicher“

Der „Verantwortliche“ ersetzt die „verantwortliche Stelle“, wie sie bisher im BDSG verwendet wurde. **Verantwortlicher ist die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet**. In unserem Zusammenhang ist dies somit die Kanzlei oder der Einzelanwalt. Die DSGVO ermöglicht auch gemeinsame Datenverarbeitungsvorgänge mehrerer Verantwortlicher gem. Art. 26 DSGVO. Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Hier muss eine detaillierte Vereinbarung abgeschlossen werden. Bei Partnerschaftsgesellschaften ist die Gesellschaft selbst Verantwortlicher. Bei BGB-Gesellschaften dürfte dies aufgrund der Stellung der Gesellschaft als Vertragspartner ebenso sein. Interessant ist dieses Thema daher besonders bei Kooperationen.

5. „Verarbeitung“

Verarbeitung ist gem. Legaldefinition **jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten**, also beispielsweise 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.

„**Einschränkung der Verarbeitung**“ ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

Bei der Frage, ob personenbezogene Daten „**automatisiert verarbeitet**“ werden, ist es egal, welche Technik Anwendung findet. In Erwägungsgrund 15 ist hierzu geregelt:

„*Um ein ernsthaftes Risiko einer Umgehung der Vorschriften zu vermeiden, sollte der Schutz natürlicher Personen technologieneutral sein und nicht von den verwendeten Techniken abhängen. Der Schutz natürlicher Personen sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung von personenbezogenen Daten, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen.*“

Ein „**Dateisystem**“ definiert Art. 4 Nr. 6 DSGVO so: „*Unter einem Dateisystem versteht die DSGVO jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig*

davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird".

Kommen also Computer, Smartphones, Kameras, Scanner oder Kopierer zum Einsatz, so kann man davon ausgehen, dass, wenn personenbezogene Daten auf diesen Geräten gespeichert und verarbeitet werden, die DSGVO Anwendung findet.

Nicht automatisiert verarbeitet werden Daten, wenn sie beispielsweise handschriftlich erfasst werden. D. h. aber nicht, dass Daten allein deshalb, weil sie handschriftlich erfasst wurden, nie unter die DSGVO fallen können: Die DSGVO gilt auch für Daten, die automatisiert „gespeichert werden sollen" gemäß Art. 2 Abs. 1 DSGVO. **Es reicht also schon die Absicht aus, dass personenbezogene Daten in ein Dateisystem aufgenommen werden sollen**.

Und was ist mit Ihren Akten? Unterliegen die nun auch der DSGVO? In Erwägungsgrund 15 ist geregelt: „(…) *Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, sollten nicht in den Anwendungsbereich dieser Verordnung fallen.*" Nun sind jedoch Anwaltsakten (oder sollten es sein) geordnet.

Selbstverständlich ist die DSGVO auch anwendbar, wenn Sie Anwaltssoftware wie beispielsweise DATEV Anwalt pro, RA Micro, AdvoLux & Co einsetzen. Das gilt auch dann, wenn die dort gespeicherten Daten aus Akten entnommen werden oder sich auf Akten beziehen. Auch dürfte davon auszugehen sein, dass Anwaltsakten – bei allen eventuellen Problemen im Detail – durchaus nach bestimmten Kriterien geordnet sind. **Man kann also davon ausgehen, dass die in der Kanzlei vorhandenen und genutzten personenbezogenen Daten unter die DSGVO fallen**.

Ist es, abgesehen von der Neuorganisation der Kanzlei, auch nötig, dass Sie Ihre **privaten Kontaktdaten oder privaten Auftritte in sozialen Netzwerken** etc. aufgrund der DSGVO überprüfen? Soweit geht die Verordnung dann doch nicht. Sie gilt gemäß Erwägungsgrund 18 nur, wenn die Daten einen Bezug zur beruflichen oder wirtschaftlichen Tätigkeit haben – rein persönliche und familiäre Dinge werden von der DSGVO nicht erfasst.

6. „Einwilligung"

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

Die Einwilligung ist eine der Möglichkeiten, die Verarbeitung personenbezogener Daten zu rechtfertigen. Einzelheiten zur Einwilligung und auch

zur Frage, was mit bestehenden Einwilligungen geschieht, sind in den Abschnitten IV. 6 und V. 1. a dargestellt.

7. „Dritter“

Jede 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, ist Dritter i. S. der DSGVO.

8. „Unternehmen“

„Unternehmen“ ist eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen. Eine „**Unternehmensgruppe**“ ist eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht.

9. „Empfänger“

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

10. „Verletzung des Schutzes personenbezogener Daten“

Eine „Verletzung des Schutzes personenbezogener Daten“ ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden

(Art. 4 Nr. 12 DSGVO). Hier geht es also um **Datenpannen**, auch „**Data Breach**“ (dazu unten ausführlich, Abschnitt IX. 2) genannt. Es geht um folgende Situation:
- Verletzung der Sicherheit (egal, ob ein Schaden eingetreten ist)
- Bezug auf personenbezogene Daten
- Negative Folgen, also:
  - Verlust (Daten sind woanders)
  - Vernichtung (Daten sind weg)
  - Veränderung (Daten sind vielleicht falsch)
  - Offenlegung (Daten sind bei dem Falschen)
  - Zugriff Unbefugter (egal, ob der genutzt wurde)

Beispiele für eine solche Datenpanne sind: personenbezogene Daten werden versehentlich an den Falschen versendet, ein erfolgreicher Hacker-Angriff findet auf die Kanzlei statt, Diebstahl von Akten oder einem Mobilgerät, oder Akte bzw Handy bleiben im Taxi versehntlich liegen. Schadcode oder Softwarefehler können ebenfalls zu Datenpannen führen.

11. Weitere Definitionen

Zu erwähnen sind noch einige weitere Definitionen, die im Hinblick auf die Anwaltskanzlei keine ganz zentrale Bedeutung haben, aber trotzdem kurz erwähnt werden sollen:
- „**Profiling**“ ist jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen (Art. 4 Nr. 4 DSGVO);
- „**Aufsichtsbehörde**“ ist eine von einem Mitgliedstaat eingerichtete unabhängige staatliche Stelle, die gem. Art. 51 DSGVO die Aufgaben der Datenschutzaufsicht übernimmt; die „**betroffene Aufsichtsbehörde**“ ist eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil
  1. der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist,
  2. diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder
  3. eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde;

– Ein „**Dienst der Informationsgesellschaft**“ ist eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates. Das heißt im Klartext: Ein Dienst der Informationsgesellschaft ist jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung. Dabei bezeichnet
  i) „**im Fernabsatz erbrachte Dienstleistung**“ eine Dienstleistung, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht wird;
  ii) „**elektronisch erbrachte Dienstleistung**“ eine Dienstleistung, die mittels Geräten für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird;
  iii) „**auf individuellen Abruf eines Empfängers erbrachte Dienstleistung**“ eine Dienstleistung die durch die Übertragung von Daten auf individuelle Anforderung erbracht wird.