

EU-Datenschutz-Grundverordnung (DSGVO): Wichtige Begriffsbestimmungen

Personenbezogene Daten, Verarbeitung, Einwilligung, Verantwortlicher, Auftragsverarbeiter etc.

Personenbezogene Daten (Art 4 Z 1)

Die Bestimmungen der DSGVO gelten für die Verarbeitung von personenbezogenen Daten natürlicher Personen.

Definitionsgemäß sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („**betreffene Person**“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Beispiele: Name, Adresse, Geburtsdatum, Bankdaten, etc.

Die Grundsätze des Datenschutzes gelten nicht für „anonyme Informationen“, dh für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Die Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, dies gilt auch für statistische oder Forschungszwecke.

Die DSGVO gilt nicht für die personenbezogenen Daten Verstorbener. Die Mitgliedstaaten können jedoch Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen.

Das österreichische Datenschutzgesetz (DSG) nützt diese Möglichkeit jedoch nicht.

Besondere Kategorien personenbezogener Daten („sensible Daten“, Art 9 Abs 1):

Das sind personenbezogene 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.

Beispiele: Fingerabdruck, Irisscan, Krankengeschichte

Verarbeitung (Art 4 Z 2)

Unter dem Begriff „Verarbeitung“ versteht die DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Beispiele: Erstellung einer Kundendatei, Aufnahme der Daten zur Erstellung einer Rechnung, Führung einer Mitarbeiterdatenbank.

Verantwortlicher (Art 4 Z 7) und Auftragsverarbeiter (Art 4 Z 8)

„Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche bzw die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

„Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet.

Beispiele: Der Unternehmer, der Kundendaten (von natürlichen Personen) zur Erstellung einer Rechnung an den Kunden erfasst, ist „Verantwortlicher“. Der externe Buchhalter, der die Rechnungsdaten für die Bilanzerstellung von diesem Unternehmer erhält und verarbeitet, ist „Auftragsverarbeiter“. Weitere Beispiele für den „Auftragsverarbeiter“: Cloud-Dienste-Anbieter, Newsletter-Management-Anbieter, IT-Datenwartungsanbieter. Steuerberater sind nach einer Entscheidung der Datenschutzbehörde keine Auftragsverarbeiter.

Empfänger (Art 4 Z 9)

Als „Empfänger“ bezeichnet die DSGVO 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.

Von dieser Definition ist auch der Auftragsverarbeiter erfasst, d.h. auch dieser gilt als „Empfänger“.

Einwilligung (Art 4 Z 11)

Als „Einwilligung“ der betroffenen Person gilt 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.

Diese Einwilligung kann schriftlich, elektronisch oder auch mündlich erfolgen, etwa auch durch Anklicken eines Kästchens auf einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder andere Erklärungen oder Verhaltensweisen, die im jeweiligen Kontext eindeutig das Einverständnis der betroffenen Person zur Datenverarbeitung signalisieren. Stillschweigen, bereits vorangekreuzte Kästchen oder Untätigkeit können keine Einwilligung darstellen. Wenn die Verarbeitung mehreren Zwecken dient, ist für jeden Zweck der Verarbeitung eine gesonderte Einwilligung nötig.

Eine „ausdrückliche“ Einwilligung ist nur bei der Verarbeitung von sensiblen Daten erforderlich.

Kind (Art 8 Abs 1)

Für die Rechtmäßigkeit der Einwilligung eines Kindes bei einem Angebot von Diensten der Informationsgesellschaft legt die DSGVO eine Altersgrenze von 16 Jahren fest.

Die EU-Mitgliedstaaten können aber niedrigere Altersgrenzen vorsehen, allerdings nicht unter das vollendete 13. Lebensjahr. Das österreichische Datenschutzgesetz (DSG) setzt diese Altersgrenze mit dem vollendeten 14. Lebensjahr fest.

Pseudonymisierung (Art 4 Z 5)

„Pseudonymisierung“ ist die Verarbeitung personenbezogener Daten in einer 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.

Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann die Risiken für die betroffenen Personen senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen. Durch die ausdrückliche Einführung der „Pseudonymisierung“ in die DSGVO ist jedoch nicht beabsichtigt, andere Datenschutzmaßnahmen auszuschließen.

Beispiel: Verschlüsselung

Dateisystem (Art 4 Z 6)

Ein „Dateisystem“ ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geographischen Gesichtspunkten geordnet geführt wird.

Das Dateisystem kann automatisiert oder manuell geführt werden (technologieneutral). Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, fallen nicht in den Anwendungsbereich der DSGVO.

Beispiel: Kundendatei (elektronisch oder in Papierform)

Gesundheitsdaten (Art 4 Z 15)

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, werden als „Gesundheitsdaten“ definiert.

Genetische Daten (Art 4 Z 13)

„Genetische Daten“ sind 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 betroffenen natürlichen Person gewonnen wurden.

Biometrische Daten (Art 4 Z 14)

„Biometrische Daten“ sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen und verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder und daktyloskopische Daten.

Neben – wie bisher – z.B. „Gesundheitsdaten“ zählen nun auch ausdrücklich „genetische Daten“ und „biometrische Daten“ zu den „besonderen Kategorien personenbezogener Daten“ (sensible Daten) und unterliegen damit strengeren Verarbeitungsvoraussetzungen.

Profiling (Art 4 Z 4)

Darunter versteht die DSGVO 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.

Das Profiling unterliegt den Vorschriften der DSGVO, wie etwa der Rechtsgrundlage für die Verarbeitung, den Datenschutzgrundsätzen, der Informations- und Auskunftspflicht und besonderen Regeln, wenn damit eine automatische Generierung von Einzelentscheidungen verbunden ist.

Beispiel: Automationsunterstützte Analyse der Kreditwürdigkeit eines Kunden.

Relevante Artikel der DSGVO: Art 4, Art 8, Art 9

Relevante Erwägungsgründe: 26ff, 51ff

Relevante Bestimmungen des DSG: § 4 Abs 4

Stand: 01.04.2022