

EU-DSGVO: Datenschutzrechte und -pflichten

Grundsätze, Rechtsgrundlagen, Pflichten des Verantwortlichen, Betroffenenrechte und Durchsetzung

Welche Rechte, Pflichten und Rechtsgrundlagen sollten Sie verstehen, um personenbezogene Daten gemäß der DSGVO rechtmäßig zu verarbeiten?

Überblick: Die EU-Datenschutz-Grundverordnung

Als Mitarbeiter eines Unternehmens, das personenbezogene Daten verarbeitet — Kundendaten, Mitarbeiterdaten, Web-Analytik, KI-Trainingsdaten — ist die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) ^[1] der Rechtsrahmen, der Ihre Arbeit regelt. Anwendbar seit dem 25. Mai 2018 basiert die DSGVO auf sieben grundlegenden **Grundsätzen** ^[tn100] (Art. 5), die verlangen, dass personenbezogene Daten rechtmäßig, nach Treu und Glauben und transparent verarbeitet werden. Jede Verarbeitung muss auf einer der sechs **Rechtsgrundlagen** ^[tn200] (Art. 6) beruhen. Verantwortliche tragen besondere **Pflichten** ^[tn300] zur Umsetzung von Datenschutz durch Technikgestaltung, zur Führung von Verzeichnissen und zur Meldung von Verletzungen. Betroffene Personen genießen umfassende **Rechte** ^[tn400] (Art. 15–22), einschließlich Auskunft, Berichtigung, Löschung und Datenübertragbarkeit. **Artikel 3 enthält zwei Anwendbarkeitstests:** Die DSGVO gilt für die Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung in der Union (unabhängig davon, ob die Verarbeitung in der Union erfolgt), und für die Verarbeitung durch nicht in der Union niedergelassene Verantwortliche oder Auftragsverarbeiter, die betroffenen Personen in der Union Waren oder Dienstleistungen anbieten oder deren Verhalten in der Union beobachten. Die bloße Erreichbarkeit einer Website aus der Union reicht nicht aus; es bedarf eines

Targeting-Nachweises (z. B. Sprache, Währung, Top-Level-Domain, EU-spezifisches Marketing). **Durchsetzung** [tn500] erfolgt durch nationale Aufsichtsbehörden, die Geldbußen von bis zu 20 Mio. EUR oder 4 % des weltweiten Jahresumsatzes verhängen können.

Grundsätze [tn100]: Art. 5 — Grundlagen der Datenverarbeitung

Artikel 5 der DSGVO legt sieben Grundsätze fest, die die Grundlage jeder rechtmäßigen Datenverarbeitung bilden. Verantwortliche müssen die Einhaltung jedes Grundsatzes im Rahmen der **Rechenschaftspflicht** [tn107] (Art. 5(2)) nachweisen. Diese Grundsätze **erfordern eine Rechtsgrundlage** [te101] aus einer der sechs **Rechtsgrundlagen** [tn200] gemäß Art. 6 [1].

- **Rechtmäßigkeit, Treu und Glauben, Transparenz** [tn101]: Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Art. 5(1)(a))
- **Zweckbindung** [tn102]: Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (Art. 5(1)(b))
- **Datenminimierung** [tn103]: Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Art. 5(1)(c))
- **Richtigkeit** [tn104]: Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige Daten unverzüglich gelöscht oder berichtigt werden (Art. 5(1)(d))
- **Speicherbegrenzung** [tn105]: Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen

Personen nur so lange ermöglicht, wie es für die Zwecke der Verarbeitung erforderlich ist (Art. 5(1)(e))

- **Integrität und Vertraulichkeit** [tn106]: Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung durch geeignete technische oder organisatorische Maßnahmen (Art. 5(1)(f))
- **Rechenschaftspflicht** [tn107]: Der Verantwortliche ist für die Einhaltung aller oben genannten Grundsätze verantwortlich und muss deren Einhaltung nachweisen können (Art. 5(2)). Artikel 24 konkretisiert dies: Der Verantwortliche muss geeignete technische und organisatorische Maßnahmen umsetzen, unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte natürlicher Personen; diese Maßnahmen sind zu überprüfen und ggf. zu aktualisieren

Rechtsgrundlagen [tn200]: Art. 6 — Rechtliche Grundlagen der Verarbeitung

Artikel 6 legt sechs Rechtsgrundlagen fest, auf denen personenbezogene Daten verarbeitet werden dürfen. Mindestens eine Grundlage muss gelten, bevor eine Verarbeitungstätigkeit beginnt. Die Wahl der Grundlage beeinflusst, welche **Rechte der betroffenen Person** [tn400] verfügbar sind, und **erfordert Schutzmaßnahmen** [te102] zum Schutz der Betroffenen [1].

- **Einwilligung** [tn201]: Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben (Art. 6(1)(a)). Die Einwilligung muss freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich abgegeben werden. Artikel 7 regelt die operativen

Anforderungen: Der Verantwortliche muss **nachweisen können**, dass die betroffene Person eingewilligt hat (Art. 7(1)); Einwilligungsersuchen müssen in verständlicher und leicht zugänglicher Form, in einfacher Sprache und klar von anderen Sachverhalten getrennt vorgelegt werden (Art. 7(2)); die betroffene Person hat das **Recht, ihre Einwilligung jederzeit zu widerrufen**, und der Widerruf muss so einfach sein wie die Erteilung (Art. 7(3)); und bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, ist zu berücksichtigen, ob die Erfüllung eines Vertrags von einer Einwilligung abhängig gemacht wird, die nicht erforderlich ist (Art. 7(4))

- **Vertragserfüllung** [tn202]: Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen (Art. 6(1)(b))
- **Rechtliche Verpflichtung** [tn203]: Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt (Art. 6(1)(c))
- **Lebenswichtige Interessen** [tn204]: Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen (Art. 6(1)(d))
- **Öffentliches Interesse** [tn205]: Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Art. 6(1)(e))
- **Berechtigte Interessen** [tn206]: Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (Art. 6(1)(f))

Besondere Kategorien personenbezogener Daten [tn250]: Art. 9 — Zusätzliche Ebene

Artikel 9 etabliert eine erhöhte Schutzebene für sensible Kategorien personenbezogener Daten. Eine gültige **Rechtsgrundlage** [tn200] nach Artikel 6 ist erforderlich, aber nicht ausreichend — Artikel 9 verlangt eine **zusätzliche Ebene für sensible Daten** [te108], bevor die Verarbeitung rechtmäßig beginnen kann. Für Organisationen, die personenbezogene Daten in KI-Training, Kundenprofiling, biometrischer Authentifizierung oder Gesundheitsanalysen verwenden, ist Artikel 9 nach Artikel 6 die folgenreichste Bestimmung. Die Verarbeitung besonderer Kategorien **auferlegt erhöhte Pflichten** [te109] dem Verantwortlichen (DSFA-Wahrscheinlichkeit, Sicherheitsmaßnahmen, ggf. DSB).

- **Definition besonderer Kategorien** [tn251] (**Art. 9(1)**): Artikel 9(1) verbietet die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen; die Verarbeitung genetischer Daten; biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person; Gesundheitsdaten; oder Daten zum Sexualleben oder zur sexuellen Orientierung. Das Verbot gilt unabhängig davon, ob eine gültige Rechtsgrundlage nach Artikel 6 vorliegt.
- **Bedingungen für die Aufhebung des Verbots** [tn252] (**Art. 9(2)**): Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur dann zulässig, wenn eine der zehn Bedingungen in Artikel 9(2) erfüllt ist. Die operationell relevantesten sind: (a) ausdrückliche Einwilligung der betroffenen Person; (b) arbeits-, sozialversicherungs- und sozialschutzrechtliche Bestimmungen; (c) lebenswichtige Interessen einer einwilligungsunfähigen Person; (e) Daten, die die betroffene Person offensichtlich öffentlich gemacht hat; (g) erhebliches öffentliches Interesse mit angemessenen Schutzmaßnahmen; (h) Vorsorgemedizin oder Arbeitsmedizin, medizinische Diagnostik oder Behandlung unter Berufsgeheimnis; (i) öffentliche Gesundheit; und (j) Archivzwecke, wissenschaftliche oder historische Forschungs- oder Statistikzwecke im öffentlichen Interesse. Mitgliedstaaten können zusätzliche Bedingungen für genetische, biometrische oder Gesundheitsdaten vorsehen (Art. 9(4)).
- **KI-Training und besondere Kategorien** [tn253]: Für Organisationen, die personenbezogene Daten für KI-Training nutzen: Jede Inferenz oder Merkmalsableitung, die eine besondere Kategorie offenbart (z. B. Ableitung von Gesundheitsstatus, sexueller Orientierung oder

politischen Meinungen aus nicht-sensiblen Eingaben), bringt die Verarbeitung in den Anwendungsbereich von Artikel 9. Pseudonymisierung allein entfernt Daten nicht aus dem Regime besonderer Kategorien; nur echte Anonymisierung (Erwägungsgrund 26) tut dies — und die Schwelle für Anonymisierung ist hoch (keine vernünftigen Mittel zur Re-Identifizierung). Die Verarbeitung besonderer Kategorien in KI-Systemen löst zudem typischerweise die DSFA-Pflicht nach Art. 35(3)(b) aus.

Pflichten des Verantwortlichen [tn300]: Wesentliche Pflichten des Verantwortlichen

Die DSGVO erlegt Verantwortlichen besondere Pflichten auf, um sicherzustellen, dass personenbezogene Daten im Einklang mit ihren **Grundsätzen** [tn100] verarbeitet werden. Diese **Pflichten schützen** [te103] die **Rechte der betroffenen Person** [tn400] und helfen, Verstöße zu verhindern, die **Durchsetzungsmaßnahmen auslösen** [te104] könnten [1].

- **Verantwortlicher vs. Auftragsverarbeiter** [tn220] (**Art. 4(7), 4(8), 26, 28**): Die DSGVO unterscheidet **Verantwortliche** (die über Zwecke und Mittel der Verarbeitung entscheiden, Art. 4(7)) und **Auftragsverarbeiter** (die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeiten, Art. 4(8)). Ein Unternehmen kann für einige Tätigkeiten Verantwortlicher sein (z. B. Verarbeitung der Mitarbeiterdaten) und für andere Auftragsverarbeiter (z. B. SaaS-Bereitstellung an Geschäftskunden). Die Unterscheidung bestimmt, wer für welche Pflichten zuständig ist: Verantwortliche tragen die Hauptverantwortung für Grundsätze und Rechte; Auftragsverarbeiter sind durch Art. 28 (Verträge), Art. 32 (Sicherheit), Art. 33 (Meldung an den Verantwortlichen) und Art. 37–39 (DSB, wo zutreffend) gebunden. Beide können unmittelbar mit Bußgeldern belegt werden. **Gemeinsam**

Verantwortliche (Art. 26) legen Zwecke und Mittel gemeinsam fest und müssen ihre jeweiligen Pflichten durch eine transparente Vereinbarung regeln, die den betroffenen Personen zugänglich gemacht wird.

- **Datenschutz durch Technikgestaltung** [\[tn301\]](#) **(Art. 25):** Der Verantwortliche muss geeignete technische und organisatorische Maßnahmen — wie Pseudonymisierung und Datenminimierung — sowohl zum Zeitpunkt der Festlegung der Mittel als auch zum Zeitpunkt der Verarbeitung selbst treffen, um sicherzustellen, dass standardmäßig nur die für den jeweiligen Zweck erforderlichen personenbezogenen Daten verarbeitet werden
- **Auftragsverarbeiter** [\[tn302\]](#) **(Art. 28):** Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, darf dieser nur Auftragsverarbeiter einsetzen, die hinreichende Garantien bieten. Die Verarbeitung durch einen Auftragsverarbeiter muss durch einen Vertrag oder ein anderes Rechtsinstrument geregelt sein, das Gegenstand, Dauer, Art und Zweck der Verarbeitung festlegt
- **Verzeichnis von Verarbeitungstätigkeiten** [\[tn303\]](#) **(Art. 30):** Jeder Verantwortliche und jeder Auftragsverarbeiter muss ein Verzeichnis aller Verarbeitungstätigkeiten führen, einschließlich der Zwecke der Verarbeitung, der Kategorien betroffener Personen und personenbezogener Daten, der Empfänger und der vorgesehenen Fristen für die Löschung
- **Meldung an die Aufsichtsbehörde** [\[tn304\]](#) **(Art. 33):** Im Falle einer Verletzung des Schutzes personenbezogener Daten muss der Verantwortliche die zuständige Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, benachrichtigen (Art. 33(1)). Erfolgt die Benachrichtigung nicht binnen 72 Stunden, sind die Gründe für die Verzögerung beizufügen. Die Meldung ist nicht erforderlich, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Die Meldung muss die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, den Namen des Datenschutzbeauftragten, die wahrscheinlichen Folgen und die ergriffenen Maßnahmen enthalten (Art. 33(3)).
- **Datenschutz-Folgenabschätzung** [\[tn305\]](#) **(Art. 35):** Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien,

voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so muss der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen

- **Benachrichtigung betroffener Personen** ^[tn311] (**Art. 34**): **Bei hohem Risiko an Betroffene** ^[te305]: Wenn eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, muss der Verantwortliche die betroffenen Personen unverzüglich benachrichtigen (Art. 34(1)). Die Benachrichtigung muss die Verletzung in klarer und einfacher Sprache beschreiben und den Namen und die Kontaktdaten des Datenschutzbeauftragten, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Maßnahmen enthalten (Art. 34(2)). Eine Benachrichtigung der betroffenen Personen ist nicht erforderlich, wenn der Verantwortliche geeignete Schutzmaßnahmen getroffen hat (z. B. Verschlüsselung, die die Daten unzugänglich macht), wenn nachfolgende Maßnahmen das hohe Risiko ausgeschlossen haben, oder wenn dies mit unverhältnismäßigem Aufwand verbunden wäre — in diesem Fall ist eine öffentliche Bekanntmachung erforderlich (Art. 34(3)).
- **Informationspflicht bei Erhebung** ^[tn306] (**Art. 13**): Werden personenbezogene Daten direkt bei der betroffenen Person erhoben, verlangt Art. 13, dass der Verantwortliche zum Zeitpunkt der Erhebung folgende Informationen bereitstellt: Identität und Kontaktdaten des Verantwortlichen; gegebenenfalls Kontaktdaten des Datenschutzbeauftragten; Verarbeitungszwecke und Rechtsgrundlage; bei berechtigtem Interesse (Art. 6(1)(f)) das verfolgte Interesse; Empfänger oder Kategorien von Empfängern; Angaben zu Drittlandübermittlungen und den dabei genutzten Schutzmaßnahmen; Speicherdauer oder Kriterien; Bestehen der Betroffenenrechte (Art. 15–22); Recht auf Widerruf der Einwilligung; Beschwerderecht bei einer Aufsichtsbehörde; ob die Bereitstellung gesetzlich oder vertraglich vorgeschrieben ist; und Bestehen einer automatisierten Entscheidungsfindung (Art. 22) einschließlich aussagekräftiger Informationen zur involvierten Logik.
- **Informationspflicht bei Drittquelle** ^[tn307] (**Art. 14**): Werden personenbezogene Daten nicht bei der betroffenen Person erhoben (z.

B. von Datenmaklern, aus öffentlichen Quellen oder von anderen Verantwortlichen), verlangt Art. 14, dass der Verantwortliche den gleichen Inhalt wie nach Art. 13 bereitstellt sowie die betreffenden Datenkategorien und die Datenherkunft. Die Informationen müssen innerhalb einer angemessenen Frist nach der Erhebung, längstens innerhalb eines Monats, oder bei der ersten Kommunikation mit der betroffenen Person, oder bei der ersten Offenlegung an Dritte bereitgestellt werden — je nachdem, was zuerst eintritt. Eingeschränkte Ausnahmen gelten, wenn die Bereitstellung unmöglich ist oder einen unverhältnismäßigen Aufwand erfordern würde (Art. 14(5)).

- **Benennung des DSB** [\[tn308\]](#) **(Art. 37):** Ein Datenschutzbeauftragter (DSB) ist zu benennen, wenn (a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird; (b) die Kerntätigkeit des Verantwortlichen oder Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, die eine umfangreiche regelmäßige und systematische Überwachung betroffener Personen erforderlich machen; oder (c) die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Datenkategorien (Art. 9) oder von Daten über strafrechtliche Verurteilungen (Art. 10) besteht. In anderen Fällen ist die Benennung freiwillig. Eine Unternehmensgruppe oder ein Verbund öffentlicher Stellen kann einen gemeinsamen DSB benennen. Die Kontaktdaten des DSB sind zu veröffentlichen und der Aufsichtsbehörde mitzuteilen (Art. 37(7)).
- **Stellung des DSB** [\[tn309\]](#) **(Art. 38):** Der DSB ist ordnungsgemäß und frühzeitig in alle Fragen einzubinden, die mit dem Schutz personenbezogener Daten zusammenhängen (Art. 38(1)); muss mit den Mitteln und dem Zugang ausgestattet werden, die zur Aufgabenerfüllung erforderlich sind (Art. 38(2)); und darf keine Anweisungen hinsichtlich der Aufgabenwahrnehmung erhalten (Art. 38(3)). Der DSB darf wegen der Aufgabenerfüllung nicht abberufen oder benachteiligt werden. Der DSB berichtet unmittelbar der höchsten Leitungsebene. Betroffene Personen können den DSB zu allen Verarbeitungsfragen und zur Wahrnehmung ihrer Rechte zu Rate ziehen (Art. 38(4)).
- **Aufgaben des DSB** [\[tn310\]](#) **(Art. 39):** Artikel 39 nennt die Kernaufgaben des DSB: Information und Beratung des Verantwortlichen, des Auftragsverarbeiters und der Beschäftigten hinsichtlich ihrer Pflichten

nach dem Datenschutzrecht; Überwachung der Einhaltung der DSGVO und der internen Vorschriften (einschließlich Zuweisung von Zuständigkeiten, Sensibilisierung, Schulung und Audits); Beratung im Zusammenhang mit Datenschutz-Folgenabschätzungen (Art. 35) auf Anfrage; Zusammenarbeit mit der Aufsichtsbehörde; und Funktion als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen (Art. 39(1)(e)).

Rechte der betroffenen Person [tn400]: Art. 15–22 — Individuelle Rechte

Die DSGVO gewährt Einzelpersonen umfassende Rechte über ihre personenbezogenen Daten. Werden diese Rechte **verweigert** [te105], können betroffene Personen Beschwerden einreichen, die **Durchsetzungsmaßnahmen** [tn500] auslösen. Eine Verarbeitung ohne gültige **Rechtsgrundlage** [te106] aus den **Rechtsgrundlagen** [tn200] stellt ebenfalls einen Verstoß dar [1]. Der Verantwortliche muss einer Anfrage einer betroffenen Person **unverzüglich, in jedem Fall aber innerhalb eines Monats** nach Eingang nachkommen (Art. 12(3)). Diese Frist kann um zwei weitere Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl der Anträge erforderlich ist; die betroffene Person ist innerhalb eines Monats über die Verlängerung und deren Gründe zu informieren.

- **Auskunftsrecht** [tn401] (**Art. 15**): Stellt ein Kunde oder Nutzer einen Auskunftsantrag, muss der Verantwortliche bestätigen, ob personenbezogene Daten über die anfragende Person verarbeitet werden, und gegebenenfalls eine Kopie der Daten sowie Informationen über die Verarbeitungszwecke, Datenkategorien und Empfänger bereitstellen (Art. 15)
- **Recht auf Berichtigung** [tn402] (**Art. 16**): Meldet ein Kunde, dass Daten über ihn unrichtig sind, muss der Verantwortliche diese unverzüglich berichtigen (Art. 16). Die betroffene Person hat zudem das Recht auf Vervollständigung unvollständiger Daten. Dieses Recht steht in

Verbindung mit dem Grundsatz der **Richtigkeit** [tn104]: sind Daten **unrichtig, müssen sie berichtigt werden** [te301]

- **Recht auf Löschung** [tn403] (**Art. 17**): Verlangt ein Kunde die Löschung seiner Daten, muss der Verantwortliche diese unverzüglich löschen (Art. 17), wenn die Daten **nicht mehr benötigt werden** [te302], die Einwilligung widerrufen wird, die betroffene Person Widerspruch einlegt oder die Daten unrechtmäßig verarbeitet wurden
- **Recht auf Einschränkung** [tn404] (**Art. 18**): Verlangt ein Kunde die Einschränkung der Verarbeitung seiner Daten, muss der Verantwortliche dies anwenden, wenn: die Richtigkeit der Daten bestritten wird (während der Überprüfung); die Verarbeitung unrechtmäßig ist, die betroffene Person aber der Löschung widerspricht; der Verantwortliche die Daten nicht mehr benötigt, die betroffene Person sie aber für Rechtsansprüche braucht; oder die betroffene Person Widerspruch eingelegt hat
- **Recht auf Datenübertragbarkeit** [tn405] (**Art. 20**): Verlangt ein Kunde seine Daten in einem übertragbaren Format, muss der Verantwortliche die von der betroffenen Person bereitgestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format bereitstellen und (sofern technisch machbar) direkt an einen anderen Verantwortlichen ihrer Wahl übermitteln (Art. 20)
- **Widerspruchsrecht** [tn406] (**Art. 21**): Erhebt ein Kunde Widerspruch gegen die Verarbeitung auf Grundlage öffentlichen Interesses oder berechtigter Interessen (Art. 6(1)(e) oder (f)), muss der Verantwortliche die Verarbeitung einstellen, sofern er nicht zwingende schutzwürdige Gründe nachweisen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen — oder die Verarbeitung der Geltendmachung von Rechtsansprüchen dient (Art. 21(1)). Betroffene Personen **können auch widersprechen** [te303], wenn die Verarbeitung zum Zweck der Direktwerbung erfolgt; in diesem Fall dürfen die Daten nicht mehr zu diesem Zweck verarbeitet werden
- **Automatisierte Entscheidungsfindung** [tn407] (**Art. 22**): Ist ein Kunde einer ausschließlich auf automatisierter Verarbeitung (einschließlich Profiling) beruhenden Entscheidung unterworfen, die rechtliche Wirkung entfaltet oder ihn ähnlich erheblich beeinträchtigt, hat er das Recht, dieser Entscheidung nicht unterworfen zu werden (Art. 22(1)), es sei denn, dies ist für einen Vertrag erforderlich, gesetzlich zugelassen oder

beruht auf ausdrücklicher Einwilligung. Sofern automatisierte Entscheidungsfindung nach Art. 22(2) zulässig ist, muss der Verantwortliche geeignete Schutzmaßnahmen treffen, darunter mindestens das **Recht auf menschliches Eingreifen**, das Recht auf Darlegung des eigenen Standpunkts und das Recht auf Anfechtung der Entscheidung (Art. 22(3)). Entscheidungen, die auf besonderen Datenkategorien beruhen, erfordern entweder ausdrückliche Einwilligung oder eine Grundlage des erheblichen öffentlichen Interesses mit Schutzmaßnahmen (Art. 22(4)). Die betroffene Person hat zudem das Recht auf **aussagekräftige Informationen über die involvierte Logik** sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung (Art. 13(2)(f), 14(2)(g), 15(1)(h))

Internationale Datenübermittlungen

[tn600]: Art. 44–49 (Kapitel V)

Kapitel V regelt die Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen. Jede grenzüberschreitende **Übermittlung erfordert Rechtsgrundlage und Garantien** [te110], um das DSGVO-Schutzniveau zu wahren. Der Mechanismus ist mehrstufig — Angemessenheitsbeschlüsse, wo vorhanden, geeignete Garantien anderenfalls, und enge Ausnahmen für Einzelfälle. Nach dem Schrems-II-Urteil des EuGH erfordern auch Übermittlungen auf Grundlage von Standardvertragsklauseln eine Übermittlungsfolgenabschätzung zur Bewertung lokaler Zugriffsrisiken. Verstöße gegen Kapitel V **lösen Tier-2-Bußgelder** [te111] nach Art. 83(5) aus.

- **Allgemeines Prinzip** [tn601] (**Art. 44**): Artikel 44 statuiert das allgemeine Prinzip: Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation ist nur unter Einhaltung der in Kapitel V niedergelegten Bedingungen zulässig. Das durch die DSGVO garantierte Schutzniveau darf nicht untergraben werden.

- **Angemessenheitsbeschlüsse** [tn602] **(Art. 45):** Übermittlungen sind zulässig, wenn die Europäische Kommission entschieden hat, dass ein Drittland, ein Gebiet oder ein bestimmter Sektor ein angemessenes Schutzniveau bietet. Bestehende Angemessenheitsbeschlüsse umfassen unter anderem das Vereinigte Königreich, die Schweiz, Japan, Südkorea und den EU-US Data Privacy Framework. Angemessenheitsbeschlüsse unterliegen einer laufenden Überprüfung durch die Kommission und können vor dem Gerichtshof der Europäischen Union angefochten werden.
- **Geeignete Garantien** [tn603] **(Art. 46):** In Ermangelung eines Angemessenheitsbeschlusses sind Übermittlungen zulässig, wenn der Verantwortliche oder Auftragsverarbeiter geeignete Garantien vorgesehen hat: von der Kommission angenommene Standardvertragsklauseln (SCCs); verbindliche interne Vorschriften (BCRs, Art. 47); genehmigte Verhaltensregeln (Art. 40) mit verbindlichen, durchsetzbaren Verpflichtungen; genehmigte Zertifizierungsmechanismen (Art. 42); oder rechtsverbindliche und durchsetzbare Instrumente zwischen Behörden. Nach dem Schrems-II-Urteil des EuGH erfordern Übermittlungen auf Grundlage von SCCs zudem eine Übermittlungsfolgenabschätzung zur Bewertung lokaler Zugriffsrisiken.
- **Verbindliche interne Datenschutzvorschriften** [tn604] **(Art. 47):** Verbindliche interne Datenschutzvorschriften (BCRs) sind interne Datenschutzregeln, die von einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, angenommen und von einer zuständigen Aufsichtsbehörde genehmigt werden. BCRs ermöglichen konzerninterne Übermittlungen ohne weitere Garantien. Der Genehmigungsprozess dauert typischerweise 12-24 Monate, und die BCRs müssen die in Artikel 47(2) genannten Elemente enthalten.
- **Ausnahmen für besondere Fälle** [tn605] **(Art. 49):** In Ermangelung eines Angemessenheitsbeschlusses oder geeigneter Garantien kann eine Übermittlung im Einzelfall, nicht systematisch, auf Grundlage einer der sieben spezifischen Ausnahmen erfolgen: ausdrückliche Einwilligung nach Risikoauflärung; Erforderlichkeit für die Erfüllung eines Vertrags mit der betroffenen Person; Erforderlichkeit aus wichtigen Gründen des öffentlichen Interesses; Erforderlichkeit zur Geltendmachung, Ausübung

oder Verteidigung von Rechtsansprüchen; Erforderlichkeit zum Schutz lebenswichtiger Interessen einwilligungsunfähiger Personen; Übermittlung aus einem öffentlichen Register; oder, eng begrenzt, bei zwingenden berechtigten Interessen (Art. 49(1) zweiter Unterabsatz).

Durchsetzung [tn500]: Rechtsbehelfe, Haftung und Geldbußen

Die DSGVO bietet betroffenen Personen und Aufsichtsbehörden mehrere Durchsetzungswege. **Pflichtverletzungen** [te107] durch Verantwortliche, die ihren **Pflichten** [tn300] nicht nachkommen, können Beschwerden, gerichtliche Maßnahmen und erhebliche Geldbußen nach sich ziehen. Ein **bei der Verarbeitung festgestelltes Risiko erfordert eine Meldung** [te304] im Rahmen der Meldepflicht bei Datenschutzverletzungen [1].

- **Beschwerde bei Aufsichtsbehörde** [tn501] (**Art. 77**): Jede betroffene Person hat das Recht, eine Beschwerde bei einer Aufsichtsbehörde einzureichen, insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt
- **Gerichtlicher Rechtsbehelf** [tn502] (**Art. 79**): Jede betroffene Person hat das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund der DSGVO zustehenden Rechte infolge einer nicht verordnungskonformen Verarbeitung ihrer personenbezogenen Daten verletzt wurden
- **Recht auf Schadenersatz** [tn503] (**Art. 82**): Jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder den Auftragsverarbeiter

- **Geldbußen: bis 10 Mio. EUR / 2% [tn504] (Art. 83(4)):** Verstöße gegen die Pflichten des Verantwortlichen und des Auftragsverarbeiters (einschließlich Art. 25, 28, 30, 33, 35), Pflichten der Zertifizierungsstelle und der Überwachungsstelle werden mit Geldbußen von bis zu 10.000.000 EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs geahndet, je nachdem, welcher Betrag höher ist
- **Geldbußen: bis 20 Mio. EUR / 4% [tn505] (Art. 83(5)):** Verstöße gegen die Grundsätze für die Verarbeitung (Art. 5–7), die Rechte der betroffenen Person (Art. 12–22), die Übermittlungsvorschriften (Art. 44–49) und die Nichtbefolgung von Anordnungen der Aufsichtsbehörde werden mit Geldbußen von bis zu 20.000.000 EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes geahndet, je nachdem, welcher Betrag höher ist

Referenzen

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L 119. [\[Source\]](#)
2. European Data Protection Board. Guidelines, Recommendations & Best Practices. [\[Source\]](#)

Häufig gestellte Fragen

F: Was ist die DSGVO?

A: Die DSGVO (Verordnung (EU) 2016/679) ist die umfassende Datenschutzverordnung der Europäischen Union, anwendbar seit dem 25. Mai 2018. Sie legt Regeln für die Verarbeitung personenbezogener Daten durch Verantwortliche und Auftragsverarbeiter fest, basiert auf sieben zentralen

Grundsätzen [tn100] (Art. 5) und sechs **Rechtsgrundlagen** [tn200] für die Verarbeitung (Art. 6) und gewährt Einzelpersonen umfassende **Rechte der betroffenen Person** [tn400].

F: Gilt die DSGVO für mein Unternehmen?

A: Artikel 3 enthält zwei Anwendbarkeitstests. Erstens gilt die DSGVO für jede Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der Union — unabhängig davon, ob die Verarbeitung selbst außerhalb der Union erfolgt (Art. 3(1)). Zweitens gilt die DSGVO für nicht in der Union niedergelassene Verantwortliche oder Auftragsverarbeiter, wenn die Verarbeitung (a) das Angebot von Waren oder Dienstleistungen an betroffene Personen in der Union betrifft, oder (b) die Beobachtung ihres Verhaltens, soweit es in der Union stattfindet (Art. 3(2)). Die bloße Erreichbarkeit einer Website aus der Union reicht nicht aus; es bedarf eines Targeting-Nachweises (z. B. Sprache, Währung, Top-Level-Domain, EU-spezifisches Marketing). Beispiele: Ein US-SaaS, das EU-Kunden adressiert — ja; ein Nicht-EU-Unternehmen ohne EU-Angebote oder Beobachtung — nein; ein in der EU niedergelassener Auftragsverarbeiter für einen Nicht-EU-Verantwortlichen — ja, für die Tätigkeiten der EU-Niederlassung.

F: Was sind die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten?

A: Artikel 6 legt sechs Rechtsgrundlagen fest: **Einwilligung** [tn201] der betroffenen Person, **Vertragserfüllung** [tn202], **rechtliche Verpflichtung** [tn203], Schutz **lebenswichtiger Interessen** [tn204], **öffentliches Interesse** [tn205] oder öffentliche Gewalt, und **berechtigte Interessen** [tn206] des Verantwortlichen oder eines Dritten. Mindestens eine Grundlage muss gelten, bevor eine Verarbeitung beginnen kann.

F: Welche Rechte haben Einzelpersonen nach der DSGVO?

A: Einzelpersonen haben sieben zentrale Rechte: **Auskunftsrecht** [tn401] (Art. 15), **Recht auf Berichtigung** [tn402] (Art. 16), **Recht auf Löschung** [tn403] (Art. 17), **Recht auf Einschränkung** [tn404] (Art. 18), **Recht auf Datenübertragbarkeit** [tn405] (Art. 20), **Widerspruchsrecht** [tn406] (Art. 21) und Schutz vor **automatisierter Entscheidungsfindung** [tn407] (Art. 22).

F: Welche Geldbußen drohen bei DSGVO-Verstößen?

A: Die Geldbußen sind nach Schwere gestaffelt. Verstöße gegen **Pflichten des Verantwortlichen** [tn300] wie **Datenschutz durch Technikgestaltung** [tn301], **Verzeichnis von Verarbeitungstätigkeiten** [tn303] und **Meldung von Verletzungen** [tn304] können zu **Geldbußen bis 10 Mio. EUR oder 2 %** [tn504] des weltweiten

Umsatzes führen. Schwerwiegendere Verstöße gegen die Verarbeitungsgrundsätze und Betroffenenrechte können zu **Geldbußen bis 20 Mio. EUR oder 4 %** [tn505] des weltweiten Umsatzes führen.

F: Was muss ein Verantwortlicher im Falle einer Datenpanne tun?

A: Gemäß Art. 33 muss der Verantwortliche die zuständige Aufsichtsbehörde über eine **Verletzung des Schutzes personenbezogener Daten** [tn304] unverzüglich und möglichst binnen 72 Stunden benachrichtigen. Führt die Verletzung voraussichtlich zu einem hohen Risiko für die Rechte von Einzelpersonen, muss der Verantwortliche auch die betroffenen Personen direkt benachrichtigen (Art. 34). Der Verantwortliche sollte auch eine **Datenschutz-Folgenabschätzung** [tn305] für risikoreiche Verarbeitungstätigkeiten durchführen und **Anforderungen an Auftragsverarbeiter** [tn302] in Verträgen festlegen.