



Die äußerst umfangreiche und kompliziert formulierte [DS-GVO](#) wird im Folgenden stark gekürzt und vereinfacht auf vier Seiten dargestellt. Es werden die wichtigsten Passagen für den **nicht-öffentlichen Bereich** („Privatwirtschaft“) auszugsweise zitiert.

Somit liefert der **PrivazyPlan®** ein wertvolles Dokument für die tägliche Arbeit mit der DS-GVO. Wollen Sie wissen, wie der PrivazyPlan® auch Ihr Unternehmen für die DS-GVO fit macht? Dann schauen Sie in unsere ausführliche [Leseprobe](#).

[Artikel 1 \(Gegenstand und Ziele\)](#)

Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

[Artikel 2 \(Sachlicher Anwendungsbereich\)](#) ... ergänzt durch § 1 BDSG-neu

Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. [Gemäß § 26 Abs. 7 BDSG-neu gilt der Datenschutz bei Beschäftigten-Daten auch auf „Schmierzetteln“ etc.]

[Artikel 4 \(Begriffsbestimmungen\)](#) ... ergänzt durch § 2 BDSG-neu

„personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann

[Artikel 5 \(Grundsätze für die Verarbeitung personenbezogener Daten\)](#)

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (\"Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“) [...] Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung **nachweisen** können (\"Rechenschaftspflicht“).

[Artikel 6 \(Rechtmäßigkeit der Verarbeitung\)](#) ... ergänzt durch §§ 22, 26, 27 BDSG-neu

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: **a)** Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben; **b)** 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; **c)** die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt; **d)** die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen; **e)** 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; **f)** die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, [...]

[Artikel 7 \(Bedingungen für die Einwilligung\)](#)

Beruhet die Verarbeitung auf einer Einwilligung, muss der Verantwortliche **nachweisen** können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. [...] Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen.

[Artikel 9 \(Besondere Kategorien „sensibler“ Daten\)](#)

Untersagt ist die Verarbeitung von Daten bezüglich rassistischer und ethnischer Herkunft, politischer Meinung, religiöser oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben/Sexualorientierung. Ausnahmen liefert Artikel 9 in den Absätzen 2-4; ergänzt durch § 22, 24, 26, 27, 28 BDSG-neu.

[Artikel 13 \(Informationspflicht bei der Erhebung von personenbezogenen Daten\)](#)

Werden personenbezogene Daten bei der betroffenen Person erhoben, so **teilt** der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes **mit**: **a)** den Namen und die Kontaktdaten des Verantwortlichen **b)** gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten; **c)** die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung; **d)** ggf. die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden; **e)** die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und **f)**

gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln [...].

Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten: **a)** die Dauer, für die die personenbezogenen Daten gespeichert werden **b)** das Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Widerspruchsrecht, Datenübertragbarkeit; **c)** ggf. das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen; **d)** das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde; **e)** ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und **f)** das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling.

Gemäß [Erwägungsgrund 62](#) entfällt die Informationspflicht unter anderem dann, wenn die Person bereits informiert ist.

[Artikel 15 \(Auskunftsrecht der betroffenen Person\)](#) ... ergänzt durch § 34 BDSG-neu

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein **Recht auf Auskunft** über diese personenbezogenen Daten und auf folgende Informationen: **a)** die Verarbeitungszwecke; **b)** die Kategorien personenbezogener Daten, die verarbeitet werden; **c)** die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind; [...]

 Der Verantwortliche stellt eine **Kopie** der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung.

[Artikel 17 \(Recht auf Löschung\)](#) ... ergänzt durch § 35 BDSG-neu

Die betroffene Person hat das Recht, von dem Verantwortlichen zu **verlangen**, dass sie betreffende personenbezogene Daten **unverzüglich gelöscht werden**, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft: [... es folgt eine lange Liste von Ausnahmen...]

[Artikel 20 \(Recht auf Datenübertragbarkeit\)](#)

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, **in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten**.

[Artikel 25 \(Technikgestaltung und datenschutzfreundliche Voreinstellungen\)](#)

Unter Berücksichtigung des Stands der Technik [...] trifft der Verantwortliche geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung —, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa **Datenminimierung** wirksam umzusetzen.

Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass **durch Voreinstellung** grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

[Artikel 28 \(Auftragsverarbeiter\)](#)

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser **nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten**, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt **auf der Grundlage eines Vertrags**, der den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.

[Artikel 30 \(Verarbeitungsverzeichnis\)](#)

Jeder Verantwortliche und gegebenenfalls sein Vertreter **führen ein Verzeichnis aller Verarbeitungstätigkeiten**, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben: a) den Namen und die Kontaktdaten des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten; b) die Zwecke der Verarbeitung; c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten; d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind; e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland f) die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien; g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

[Artikel 32 \(Sicherheit der Verarbeitung\)](#) ... ergänzt durch § 22 Abs. 2 BDSG-neu hinsichtlich „sensibler“ Daten

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein **dem Risiko angemessenes Schutzniveau zu gewährleisten**;

Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, **diese nur auf Anweisung des Verantwortlichen verarbeiten**, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

[Artikel 33 \(Meldung von Datenschutz-Verletzungen\)](#)

Der Verantwortliche **dokumentiert** Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

Im Falle einer Verletzung des Schutzes personenbezogener Daten **meldet** der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde, **es sei denn**, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich **nicht zu einem Risiko** für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

[Artikel 34 \(Benachrichtigung an betroffene Personen über Datenschutz-Verletzung\)](#) ... ergänzt durch § 29 BDSG-neu

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich **ein hohes Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so **benachrichtigt** der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

Die Benachrichtigung der betroffenen Person ist **nicht erforderlich**, wenn eine der folgenden Bedingungen erfüllt ist: **a)** der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung; **b)** der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko aller Wahrscheinlichkeit nach nicht mehr besteht; **c)** dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

[Artikel 35 \(Datenschutz-Folgenabschätzung\)](#)

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung **voraussichtlich ein hohes Risiko** für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine **Abschätzung der Folgen** der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung **den Rat des Datenschutzbeauftragten**, sofern ein solcher benannt wurde, ein. [Gemäß § 38 Abs. 1 BDSG-neu führt eine Datenschutz-Folgenabschätzung immer dazu, dass ein Datenschutzbeauftragter benannt werden muss.]

[Artikel 37 \(Benennung eines Datenschutzbeauftragten\)](#) ... ergänzt durch § 38 BDSG-neu

Der Verantwortliche benennt auf jeden Fall einen Datenschutzbeauftragten, wenn **a)** die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, **b)** die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder **c)** die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.

Der Datenschutzbeauftragte wird auf der Grundlage seiner **beruflichen Qualifikation** und insbesondere des **Fachwissens** benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.

Der Verantwortliche oder der Auftragsverarbeiter **veröffentlicht** die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

[Gemäß § 38 Abs. 1 BDSG-neu führt eine Datenschutz-Folgenabschätzung immer dazu, dass ein Datenschutzbeauftragter benannt werden muss; außerdem besteht eine Benennungspflicht bei mindestens 10 Beschäftigten.]

[Artikel 38 \(Stellung des Datenschutzbeauftragten\)](#)

Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen **eingebunden** wird.

Der Verantwortliche und der Auftragsverarbeiter **unterstützen** den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben.

Der Verantwortliche stellt sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben **keine Anweisungen** bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben **nicht abberufen** oder benachteiligt werden. Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene.

Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen **zu Rate ziehen**.

Der Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der **Vertraulichkeit** gebunden.

Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten **nicht zu einem Interessenkonflikt** führen

[Artikel 39 \(Aufgaben des Datenschutzbeauftragten\)](#)

Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben: **a) Unterrichtung und Beratung des Verantwortlichen** und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten; **b) Überwachung** der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen; **c) Beratung** — auf Anfrage — im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35; **d) Zusammenarbeit** mit der Aufsichtsbehörde; **e) Tätigkeit** als Anlaufstelle für die Aufsichtsbehörde.

[Artikel 44 \(Allgemeine Grundsätze der Datenübermittlungen in Drittländer – also Länder außerhalb der EU\)](#)

Jedwede Übermittlung personenbezogener Daten, die nach ihrer Übermittlung an ein **Drittland** verarbeitet werden sollen, **ist nur zulässig**, wenn der Verantwortliche die in diesem Kapitel V niedergelegten Bedingungen einhalten werden. Alle Bestimmungen dieses Kapitels V sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

[Artikel 77 \(Recht auf Beschwerde\)](#)

Jede betroffene Person hat das **Recht auf Beschwerde bei einer Aufsichtsbehörde**, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.

[Artikel 82 \(Recht auf Schadenersatz\)](#)

 Jede Person, die wegen eines Verstoßes gegen diese Verordnung **ein materieller oder immaterieller Schaden** entstanden ist, hat Anspruch auf Schadenersatz.

Der Verantwortliche wird von der Haftung befreit, wenn er **nachweist**, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

 Sind mehrere Verantwortliche bzw. auch Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie für den verursachten Schaden verantwortlich, so **haftet jeder** Verantwortliche oder jeder Auftragsverarbeiter **für den gesamten Schaden**, damit ein wirksamer Schadenersatz für die betroffene Person sichergestellt ist.

[Artikel 83 \(Allgemeine Bedingungen für die Verhängung von Geldbußen\)](#) ... ergänzt durch §§ 41, 42, 43 BDSG-neu

Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung **in jedem Einzelfall wirksam, verhältnismäßig und abschreckend** ist.

Geldbußen werden je nach den Umständen des Einzelfalls verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt: **a)** Art, Schwere und Dauer des Verstoßes **b)** Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes; **c)** jegliche getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens; [...]

 Bei Verstößen gegen die folgenden Bestimmungen werden Geldbußen von bis zu **10 Mio. EUR** oder im Fall eines Unternehmens von bis zu **2 %** seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist: Artikel 8, 11, 25 bis 39, 42 und 43.

 Bei Verstößen gegen die folgenden Bestimmungen werden Geldbußen von bis zu **20 Mio. EUR** oder im Fall eines Unternehmens von bis zu **4 %** seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist: Artikel 5-7, 9, 12-22, 44-49, 58 und Kapitel IX (nationale Rechtsvorschriften).

[Artikel 88 \(Datenverarbeitung im Beschäftigungskontext\)](#) ... ergänzt durch § 26 BDSG-neu

Die Mitgliedstaaten können spezifischere Vorschriften zur Gewährleistung des Schutzes von Beschäftigendendaten vorsehen. [Dies wird durch [§ 26 BDSG-neu](#) in die Tat umgesetzt.]

 Sonstige wichtige Aspekte im neuen Bundesdatenschutzgesetz: [§ 7](#) (Videoüberwachung), [§ 26](#) (Beschäftigungsverhältnis), [§§ 30, 31](#) (Verbraucherkredite und Scoring), [§ 38](#) (Datenschutzbeauftragter), [§ 42](#) (Strafvorschriften: **Bis zu 3 Jahre Haftstrafe**) und [§ 43](#) (Bußgeld).