



Datenschutz-Grundverordnung (DS-GVO)

FAQ für Verwaltung, Personal und Vertrieb / Marketing

Sehr geehrte*r Leser*in,

die Datenschutz-Grundverordnung (DS-GVO) stellt Unternehmen auch Jahre nach ihrer Einführung vor immer neue Herausforderungen – insbesondere in den Bereichen Verwaltung, Personal sowie Vertrieb und Marketing. Rechtsprechung und Aufsichtsbehörden liefern laufend neue Impulse, während digitale Technologien wie Künstliche Intelligenz zusätzliche datenschutzrechtliche Fragen aufwerfen.

Dieses Whitepaper greift die praxisrelevantesten Fragen aus dem betrieblichen Alltag auf und beantwortet sie so klar und verständlich wie möglich. Zugleich finden Sie zu jeder Antwort den zugehörigen rechtlichen Hintergrund. Bitte beachten Sie, dass pauschale Antworten im Datenschutzrecht nicht immer möglich sind und im Zweifel stets der oder die zuständige Datenschutzbeauftragte hinzuzuziehen ist.

Diese aktualisierte Fassung berücksichtigt Entwicklungen bis April 2026, darunter:

- Die Standardvertragsklauseln der EU-Kommission (2021) und aktuelle Drittlandtransfers nach Schrems II
- Das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) und aktuelle CookieRechtsprechung
- Den EU AI Act und seine datenschutzrechtlichen Implikationen
- Aktuelle EuGH- und BGH-Entscheidungen zu Betroffenenrechten und Schadensersatz

Wir wünschen Ihnen viel Freude beim Lesen.



Inhalt

Vorwort	2
Inhalt	3
01 Auftragsverarbeitung	4
02 Pflichtinformationen nach Art. 13 und 14 DS-GVO	5
03 Umgang mit Bewerberdaten	6
04 Werbliche Nutzung personenbezogener Daten in Vertrieb und Marketing	7
05 Veröffentlichung von Bildern im Internet	8
06 Löschung von Daten	9
07 E-Mail-Postfach und Software	10
08 Einsatz von Cookies	11
09 Künstliche Intelligenz und Datenschutz (NEU)	12
10 Betroffenenrechte und Schadensersatz (aktualisiert)	13
Schlussbemerkung.....	14

01 Auftragsverarbeitung

Wann ist ein Auftragsverarbeitungsvertrag abzuschließen?

Antwort: Wenn der Dienstleister ein Auftragsverarbeiter im Sinne von Art. 28 DS-GVO ist.

Bei der Einschaltung von Dienstleistern kann es sein, dass das Thema Auftragsverarbeitung relevant wird. Hierbei handelt es sich um eine datenschutzrechtliche Sonderkonstellation, die vertraglich besonders ausgestaltet werden muss. Wann eine solche Situation vorliegt, ist nicht immer eindeutig.

Typische Fälle der Auftragsverarbeitung sind:

- Call Center
 - Marktforschungsinstitute
 - Letter-Shop / Mailing
 - IT-Support und sonstige Dienstleistungen, bei denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann
 - IT-Outsourcing
 - Application-Service-Providing / Cloud Computing
 - Externe Personalverwaltung
 - Datenvernichtung (Akten oder Datenträger)
 - Digitalisierung von Dokumenten
-
- Keine Auftragsverarbeitung liegt hingegen in folgenden Fällen vor:
 - Reisebüro
 - Bildungsanbieter
 - Hausmeister
 - Reinigungsunternehmen
 - Post- und Versanddienstleister
 - Telekommunikationsdienstleister
 - Bank

Vor Abschluss eines Auftragsverarbeitungsvertrages sind die technischen und organisatorischen Maßnahmen (TOM) des jeweiligen Auftragsverarbeiters zu prüfen und zu dokumentieren. Regelmäßige Überprüfungen der TOM sind Pflicht.

Rechtlicher Hintergrund: Art. 28 DS-GVO regelt die Auftragsverarbeitung. Der Auftragsverarbeiter unterliegt vollumfänglich den Weisungen des Verantwortlichen. Im Vertrag müssen Gegenstand, Dauer, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten sowie Pflichten und Rechte des Verantwortlichen festgehalten werden.

Ist mit dem Steuerberater ein Auftragsverarbeitungsvertrag zu schließen?

Antwort: Es kommt darauf an.

Ist der Steuerberater lediglich im Rahmen einer externen Lohn- und Gehaltsbuchhaltung tätig, handelt er weisungsgebunden und gilt als Auftragsverarbeiter. Erbringt er hingegen originäre Steuerberatungsleistungen, ist er als eigenständiger Dritter anzusehen – ein gesonderter Auftragsverarbeitungsvertrag ist dann nicht erforderlich.

02 Pflichtinformationen nach Art. 13 und 14 DS-GVO

Müssen Bestandskunden eine Datenschutzerklärung erhalten?

Antwort: Nein.

Eine Datenschutzerklärung gibt es nur im telemedienrechtlichen Umfeld (Webseiten und Apps). Was Unternehmen ihren Kund*innen schicken sollten, sind die Pflichtinformationen nach Art. 13 DS-GVO. Diese müssen zum Zeitpunkt der Datenerhebung bereitgestellt werden – nicht nachträglich.

① Hinweis: Das massenhafte Versenden von Datenschutzerklärungen an Bestandskund*innen zur Unterschrift ist nicht erforderlich und führt zu Verwirrung. Es handelt sich nicht um ein Einwilligungsdokument, sondern um eine reine Information.

Wann müssen die Pflichtinformationen mitgeteilt werden?

Antwort: Zum Zeitpunkt der Erhebung.

Empfehlungen für die Praxis:

- Neukundin oder Neukunde über Messe: Aushang mit Pflichtinformationen vor Ort
- E-Mail-Kommunikation: Hinweis mit Link in der E-Mail-Signatur
- Online-Formular: Pflichtinformationen direkt auf der Webseite einbinden (z. B. www.unternehmen.de/datenschutz)
- Bewerbungen: Hinweis in der Eingangsbestätigung

Rechtlicher Hintergrund: Art. 13 DS-GVO gilt bei Direkterhebung, Art. 14 DS-GVO bei Dritterhebung. Die Informationspflicht besteht unabhängig vom B2B- oder B2C-Kontext.

Müssen die Pflichtinformationen unterschrieben werden?

Antwort: Nein.

Es handelt sich um eine reine Information. Ein Einverständnis oder eine Unterschrift ist weder vorgeschrieben noch rechtlich sinnvoll.

03 Umgang mit Bewerberdaten

Darf man beim alten Arbeitgeber Informationen über eine*n Bewerber*in einholen?

Antwort: Nein.

Solche Rückfragen beim früheren Arbeitgeber sind unzulässig – außer wenn der*die Bewerber*in eine konkrete Kontaktperson als Referenz mit Einwilligung angegeben hat.

Dürfen potenzielle Mitarbeitende über soziale Netzwerke angeschrieben werden?

Antwort: Nein.

Unaufgeforderte Kontaktaufnahme via LinkedIn, XING oder ähnlichen Plattformen stellt Werbung mittels elektronischer Post dar und erfordert eine vorherige ausdrückliche Einwilligung (§ 7 Abs. 2 Nr. 3 UWG). Plattformen wie LinkedIn und XING bieten jedoch eigene Opt-in-Mechanismen (z. B. LinkedIn Talent Solutions), über die Nutzende ihre Bereitschaft zur Kontaktaufnahme erklären können.

Dürfen über Bewerber*innen ergänzende Informationen im Internet eingeholt werden?

Antwort: Eingeschränkt ja – mit Fingerspitzengefühl.

Folgende Faustformel kann als Orientierung dienen:

- LinkedIn und XING: grundsätzlich zulässig (beruflicher Kontext)
- Facebook und Foren: grundsätzlich unzulässig (privater Kontext)
- Google: Einzelfallbeurteilung erforderlich

Nicht unter das Fragerecht des Arbeitgebers fallen Fragen zu Schwangerschaft, Kinderwunsch, Religion, sexueller Identität oder Behinderungen.

Rechtlicher Hintergrund: Rechtsgrundlage für Hintergrundprüfungen ist Art. 6 Abs. 1 f) DS-GVO (berechtigtes Interesse). Eine Interessenabwägung ist zwingend vorzunehmen. Vorrang hat § 26 BDSG für Daten, die zur Begründung des Beschäftigungsverhältnisses erforderlich sind.

04 Werbliche Nutzung personenbezogener Daten in Vertrieb und Marketing

Was gilt als Werbung?

Antwort: Alles, was auch nur indirekt der Absatzförderung dient.

Darunter fallen Angebote, Veranstaltungseinladungen, Feedbackanfragen, Kundenzufriedenheitsumfragen und auch Geburtstagswünsche. Selbst ein Firmenlogo mit werblicher Aufmachung gilt als Werbung.

Darf man eine Visitenkarte elektronisch speichern?

Antwort: Ja.

Das Einpflegen von Visitenkartendaten in ein CRM oder Outlook ist zulässig. Die DS-GVO ist anwendbar, die Speicherung ist aber auch ohne Einwilligung möglich, da es sich um einen Geschäftsbrauch handelt (Art. 6 Abs. 1 f) DS-GVO).

Darf man E-Mails mit werblichem Inhalt versenden?

Antwort: Grundsätzlich nur mit Einwilligung.

Das Versenden werblicher E-Mails ohne ausdrückliche Einwilligung ist unzulässig (§ 7 Abs. 2 Nr. 3 UWG). Die Übergabe einer Visitenkarte stellt keine Einwilligung dar.

 **Neu seit letzter Fassung:** Die lange geplante EU-E-Privacy-Verordnung ist noch nicht in Kraft getreten. Sobald sie gilt, werden die Anforderungen an die Einwilligung für elektronische Kommunikation überarbeitet. Die aktuellen Regelungen des UWG bleiben bis dahin maßgeblich. Es empfiehlt sich, Einwilligungen bereits jetzt rechtskonform und dokumentiert einzuholen.

Kann man Post mit werblichem Inhalt versenden?

Antwort: Ja, bis die betroffene Person widerspricht.

Postwerbung ohne Einwilligung ist wettbewerbsrechtlich nicht untersagt, solange die Betroffenen einem Werbewiderspruch nachkommen können.

Ist Telefonwerbung zulässig?

Antwort: Es kommt auf den Kontext an.

Im B2C-Bereich: nur mit ausdrücklicher Einwilligung. Im B2B-Bereich: mutmaßliche Einwilligung genügt, wenn ein sachliches Interesse angenommen werden kann (z. B. bestehende Geschäftsverbindung).

Rechtlicher Hintergrund: § 7 Abs. 2 Nr. 2 UWG; die mutmaßliche Einwilligung im B2B-Bereich ist anhand konkreter Umstände zu beurteilen.

05 Veröffentlichung von Bildern im Internet

Brauche ich eine Einwilligung für die Veröffentlichung von Fotos im Internet?

Antwort: Grundsätzlich ja.

Jede Person hat das Recht am eigenen Bild und kann entscheiden, ob und wie dieses veröffentlicht wird. Ausnahmen bestehen bei Gruppenbildern, bei denen keine einzelne Person im Fokus steht.

Was gilt für Mitarbeitendenfotos?

Antwort: Immer Einwilligung erforderlich.

Auch wenn das Foto bereits in der HR-Datenbank hinterlegt ist, muss eine separate Einwilligung für die Veröffentlichung eingeholt werden. Eine Generaleinwilligung für alle Fotos der Belegschaft ist möglich, wenn alle Voraussetzungen (Information, Bestimmtheit, Freiwilligkeit) erfüllt sind.

Was passiert, wenn eine beschäftigte Person die Einwilligung widerruft?

Antwort: Die Bilder müssen aus allen Medien (Webseite, Social Media etc.) entfernt werden.

① *Hinweis: Dokumentieren Sie Einwilligungen und deren Widerruf immer schriftlich oder in einer nachvollziehbaren Form.*

06 Löschung von Daten

Muss man die Löschung von Daten dokumentieren?

Antwort: Ja, aber nicht als Einzelnachweis jedes Datensatzes.

Die DS-GVO schreibt keine Dokumentation der Löschung einzelner Datensätze vor. Ausreichend sind:

- Technisch hinterlegte Löschkonzepte und Fristen in der eingesetzten Software
- Löschzertifikate oder Protokolle externer Dienstleister (mit Datum, Medium und Verfahren)
- Nachweis der regelmäßigen Überprüfung des Löschkonzepts

 **Neu seit letzter Fassung: Aktuelle EuGH-Rechtsprechung (C-200/23) bestätigt, dass eine unzulässige Datenspeicherung über die festgelegte Löschfrist hinaus einen immateriellen Schaden begründen kann, der zu Schadensersatzansprüchen führt. Löschkonzepte sind daher kein optionales Instrument, sondern Pflicht.**

07 E-Mail-Postfach und Software

Ist die Einsicht in E-Mail-Postfächer von Mitarbeitenden erlaubt?

Antwort: Es kommt auf die Nutzungsregelung an.

- Privatnutzung erlaubt: Einsicht ohne Einwilligung grundsätzlich unzulässig
- Privatnutzung verboten: Einsicht grundsätzlich zulässig

Die Einsicht ist zwingend mit dem oder der Datenschutzbeauftragten abzustimmen.

Ist veraltete Software ein Datenschutzproblem?

Antwort: Ja.

Software, die personenbezogene Daten verarbeitet, muss die Grundsätze des Privacy by Design und Privacy by Default einhalten (Art. 25 DS-GVO). Anforderungen:

- Datenminimierung: Nur notwendige Daten dürfen abgefragt werden
- Betroffenenrechte: Berichtigung, Löschung, Portabilität und Einschränkung müssen technisch möglich sein
- Zugriffskontrolle: Nur autorisierte Personen dürfen auf personenbezogene Daten zugreifen

Was ist beim konzernweiten Einsatz von IT-Systemen zu beachten?

Antwort: Eine Einzelfallprüfung ist zwingend erforderlich.

Die DS-GVO kennt kein Konzernprivileg. Jede Datenübermittlung zwischen Konzerngesellschaften ist gesondert auf ihre Zulässigkeit zu prüfen. Zunächst ist zu klären, ob eine gemeinsame Verantwortlichkeit (Art. 26 DS-GVO) oder eine Auftragsverarbeitung (Art. 28 DS-GVO) vorliegt.

① Hinweis: Greift eine Konzerngesellschaft außerhalb der EU oder des EWR – z. B. aus den USA – auf ein CRM zu, müssen geeignete Garantien für den Drittlandtransfer sichergestellt sein.

📌 Neu seit letzter Fassung: Nach dem Schrems-II-Urteil des EuGH (C-311/18) sind die US-Standardvertragsklauseln der EU-Kommission (SCC, Fassung 2021) das zentrale Instrument für rechtskonforme Datentransfers in die USA. Seit Juli 2023 gilt zusätzlich der EU-U.S. Data Privacy Framework (DPF) als Angemessenheitsbeschluss für zertifizierte US-Unternehmen. Ob der DPF dauerhaft Bestand hat, ist politisch noch nicht abschließend gesichert.

Rechtlicher Hintergrund: Erwägungsgrund 48 DS-GVO erkennt berechnete Interessen innerhalb einer Unternehmensgruppe an, hebt jedoch ausdrücklich hervor, dass dies die grundsätzlichen Anforderungen für Drittlandübermittlungen nicht aufhebt.

08 Einsatz von Cookies

Ist das Setzen von Cookies nach DS-GVO erlaubt?

Antwort: Grundsätzlich gilt das TTDSG, nicht primär die DS-GVO.

Seit dem 1. Dezember 2021 regelt das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) das Setzen von Cookies. Gemäß § 25 Abs. 1 TTDSG müssen Webseitenbesucher*innen grundsätzlich einwilligen. Eine Ausnahme besteht nur für technisch unbedingt erforderliche Cookies (z. B. Session-Cookies).

Eine Einwilligung ist insbesondere erforderlich für:

- Tracking- und Marketing-Cookies
- Analytische Cookies
- Funktionale Cookies, die das Nutzungsverhalten personalisieren

 **Neu seit letzter Fassung: Der Europäische Datenschutzausschuss (EDSA) hat 2023 seine Leitlinien zu Cookie-Bannern verschärft. Dark Patterns – also gestalterische Tricks, die Nutzer*innen zu einer Einwilligung verleiten – sind ausdrücklich untersagt. Ein Cookie-Banner muss das Ablehnen genauso einfach machen wie das Akzeptieren. Mehrere Aufsichtsbehörden (u. a. in Frankreich, Deutschland und Österreich) haben dies mit Bußgeldern durchgesetzt.**

Sind DS-GVO und TTDSG gleichzeitig zu beachten?

Antwort: Ja – beide Gesetze greifen ineinander.

Das TTDSG regelt das Setzen des Cookies bzw. den Zugriff auf das Endgerät. Die DS-GVO – konkret Art. 6 Abs. 1 – regelt die darauf folgende Weiterverarbeitung der gewonnenen Daten. In der Praxis können beide Einwilligungen in einer einzigen Handlung eingeholt werden, sofern der Cookie-Banner transparent über alle Zwecke informiert.

09 Künstliche Intelligenz und Datenschutz (NEU)

 **Neu seit letzter Fassung: Der EU AI Act (Verordnung (EU) 2024/1689) ist am 1. August 2024 in Kraft getreten und wird stufenweise angewendet. Er ergänzt die DS-GVO und stellt zusätzliche Anforderungen an den Einsatz von KI-Systemen, die personenbezogene Daten verarbeiten.**

Was müssen Unternehmen beim Einsatz von KI-Systemen datenschutzrechtlich beachten?

Antwort: Einiges – je nach Risikoklasse des KI-Systems.

Grundlegende Anforderungen aus DS-GVO-Sicht beim KI-Einsatz:

- Rechtsgrundlage: Auch beim KI-Einsatz muss eine Rechtsgrundlage gemäß Art. 6 DS-GVO vorliegen
- Transparenz: Betroffene müssen über automatisierte Entscheidungen informiert werden (Art. 13, 14 DS-GVO)
- Profiling: Automatisierte Entscheidungen mit erheblichen Auswirkungen bedürfen einer besonderen Rechtsgrundlage (Art. 22 DS-GVO)
- Datenschutz-Folgenabschätzung (DSFA): Bei hochriskanten KI-Systemen ist eine DSFA gemäß Art. 35 DS-GVO durchzuführen
- Datenminimierung: KI-Trainings- und Inferenzdaten dürfen nicht über den Zweck hinaus verarbeitet werden

Dürfen personenbezogene Daten in KI-Tools (z. B. ChatGPT, Microsoft Copilot) eingegeben werden?

Antwort: Grundsätzlich nur, wenn eine Rechtsgrundlage und ein Auftragsverarbeitungsvertrag vorliegen.

Vor dem Einsatz cloudbasierter KI-Dienste ist zu prüfen:

- Liegt ein Auftragsverarbeitungsvertrag mit dem Anbieter vor?
- Ist der Anbieter in einem sicheren Drittland ansässig oder liegen geeignete Garantien vor?
- Werden die Daten für das KI-Training des Anbieters genutzt? Wenn ja, ist eine Einwilligung erforderlich.

 **Hinweis:** Geben Sie keine personenbezogenen Daten (Namen, Adressen, Gesundheitsdaten etc.) in KI-Tools ein, für die kein Auftragsverarbeitungsvertrag besteht. Sprechen Sie im Zweifel Ihren oder Ihre Datenschutzbeauftragte*n an.

10 Betroffenenrechte und Schadensersatz (aktualisiert)

Welche Rechte haben betroffene Personen?

Antwort: Umfangreiche Rechte, die aktiv gewährt werden müssen.

Die DS-GVO gewährt betroffenen Personen folgende Kernrechte:

- Auskunftsrecht (Art. 15 DS-GVO): Kopie aller gespeicherten Daten
- Berichtigungsrecht (Art. 16 DS-GVO): Korrektur unrichtiger Daten
- Löschungsrecht / Recht auf Vergessenwerden (Art. 17 DS-GVO)
- Einschränkung der Verarbeitung (Art. 18 DS-GVO)
- Datenübertragbarkeit (Art. 20 DS-GVO)
- Widerspruchsrecht (Art. 21 DS-GVO), insbesondere gegen Direktwerbung

 **Neu seit letzter Fassung: Der EuGH hat in mehreren Urteilen (u. a. C-300/21, C-687/21) bestätigt, dass bereits ein Verstoß gegen die DS-GVO einen immateriellen Schadensersatzanspruch begründen kann – auch ohne nachgewiesenen konkreten Schaden. Voraussetzung ist jedoch ein tatsächlicher Verstoß und ein kausaler Zusammenhang. Unternehmen sollten Betroffenenanfragen daher stets fristgerecht (innerhalb von 30 Tagen, Art. 12 DS-GVO) und vollständig bearbeiten.**

Rechtlicher Hintergrund: Art. 82 DS-GVO regelt den Schadensersatz. Die Beweislastumkehr zugunsten der betroffenen Person bedeutet, dass Unternehmen nachweisen müssen, dass sie nicht schuldhaft gehandelt haben.

Schlussbemerkung

Das Datenschutzrecht ist ein dynamisches Rechtsgebiet. Urteile, Aufsichtsbehörden-Empfehlungen und neue Technologien verändern die Anforderungen laufend. Dieses Whitepaper bietet eine Orientierung für die Praxis, ersetzt jedoch keine individuelle Rechtsberatung.

Bei Fragen zu den genannten Themen empfehlen wir:

- Die Hinzuziehung Ihres oder Ihrer betrieblichen Datenschutzbeauftragten
- Den Austausch mit einer spezialisierten Kanzlei für Datenschutzrecht
- Die regelmäßige Teilnahme an Weiterbildungen zu aktuellen datenschutzrechtlichen Entwicklungen

Passende Weiterbildungen finden Sie hier:

Weiterbildung zum Thema Recht

Finden Sie aus unserem erstklassigen Weiterbildungsangebot die für Ihre Bedürfnisse passende Fortbildung. Profitieren Sie von unseren maßgeschneiderten Seminaren und Lehrgängen mit erfahrenen, hochkarätigen Experten rund um das Thema Recht. [Jetzt informieren.](#)

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen. [Jetzt unverbindlich testen.](#)

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als [Inhouse-Training](#). Jetzt individuelles [Angebot anfordern](#).

Wir garantieren fachlich hochwertige Weiterbildung für Ihren Erfolg – unsere ISO-Zertifizierungen nach 9001 und 21001 unterstreichen dies. [Jetzt informieren](#)