

DATENSCHUTZ – D07

Stand: August 2023

Ihr Ansprechpartner
Ass. iur. Kim Pleines
E-Mail
kim.pleines@saarland.ihk.de
Tel.
(0681) 9520-640
Fax
(0681) 9520-690

Die Datenschutzerklärung nach der DSGVO

Jeder Webseitenbetreiber verarbeitet personenbezogene Daten. Dazu gehören in der Regel:

- Name und Anschrift
- Daten über das Surfverhalten wie Suchanfragen und Browserverlauf
- IP-Adressen und sonstige User-Daten
- E-Mail-Adressen
- Daten, die mithilfe von Tracking-Software entstehen
- Bestellverlaufs-Daten

Nach **Art. 13, 14 DSGVO** ist der Betreiber der Webseite verpflichtet, der betroffenen Person, also dem Seitenbesucher, **über die Datenverarbeitung zum Zeitpunkt der Erhebung der Daten zu informieren**.

Form

Die Informationen nach Art. 13, 14 DSGVO sind in **präziser, transparenter, verständlicher und leicht zugänglicher Form** in einer **klaren und einfachen Sprache** zur Verfügung zu stellen. Bei Webseiten erfolgt das regelmäßig in der Datenschutzerklärung, die an zentraler Stelle jederzeit eingesehen werden kann und über alle datenschutzrelevanten Umstände informiert.

→ **D05** „[Informationspflichten nach der DSGVO](#)“, [Kennzahl 2356](#)

Im Onlinehandel ist es ausreichend, dass die Datenschutzerklärung mit **maximal zwei Klicks** erreichbar ist. Es empfiehlt sich ein eigener Link, welcher von sämtlichen Seiten aus anklickbar ist. Der Link sollte klar bezeichnet werden, etwa mit „Datenschutzerklärung“ oder „Datenschutz“. Nicht ausreichend ist das „Verstecken“ in den AGB. Die konkrete Ausgestaltung der Datenschutzerklärung hängt im Wesentlichen davon ab, welche Daten erhoben werden.

Achtung: Die Informationspflichten nach Art. 13, 14 DSGVO müssen auch im stationären Einzelhandel oder bei der Erbringung von Werk- oder Dienstleistungen erfüllt werden. Hier bietet es sich z.B. an, die Informationen bei der Vertragsanbahnung als Infoblatt im Ladengeschäft bereit zu halten/auszuhängen. Auch die elektronische Übermittlung der Informationen ist möglich.

Sofern im „stationären Bereich“ alle Informationen in der Datenschutzerklärung auf der Unternehmens-Homepage gegeben werden, sollte in der **Geschäftskorrespondenz** auf diese Datenschutzerklärung hingewiesen werden. Dies kann im Rahmen des Geschäftsbriefes erfolgen, indem etwa in die Fußzeile darauf hingewiesen wird, dass die Datenschutzerklärung unter der Unternehmens-Homepage www.xyz.com, unter der Rubrik „ABC“ einsehbar ist.

Auch im **E-Mail-Verkehr** kann und sollte auf die Datenschutzerklärung hingewiesen werden, etwa mit folgender Formulierung: *Gerne informieren wir Sie, ob und welche Daten wir über Sie und Ihr Unternehmen erheben. Genauere Informationen finden Sie auf unserer Homepage www.xyz.com, unter der Rubrik „ABC“.* Eine Musterformulierung enthält unser Infoblatt:

→ **GR24** „[Angaben auf Geschäftsbriefen](#)“, [Kennzahl 70](#)

Die Informationen können auch in Kombination **mit standardisierten Bildsymbolen** bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln.

Inhalt der Datenschutzerklärung

Welche Informationen bereit zu stellen sind, ergibt sich aus Art. 13, 14 DSGVO.

→ **D05** „[Informationspflichten nach der DSGVO](#)“, [Kennzahl 2356](#)

1. Identität der verantwortlichen Stelle

Die Namen und Kontaktdaten des Verantwortlichen (Name des Unternehmens/Firma, Adresse - Hausanschrift - und mindestens E-Mail-Adresse) müssen angegeben werden. Gegebenenfalls sind auch die Kontaktdaten des Vertreters (Name z. B. des Geschäftsführers, Prokuristen, Komplementärs, Adresse und mindestens E-Mail-Adresse) zu veröffentlichen. Ein Verweis auf das Impressum reicht nicht aus.

2. Kontaktdaten des Datenschutzbeauftragten

Soweit das Unternehmen rechtlich dazu verpflichtet ist, einen betrieblichen Datenschutzbeauftragten zu bestellen, sind seine Kontaktdaten zu veröffentlichen (Name, Telefonnummer, E-Mail-Adresse; wenn extern: Adresse, Firma). Bestellt das Unternehmen freiwillig einen Datenschutzbeauftragten, ist dieser ebenfalls anzugeben.

→ **D06** „[Betrieblicher Datenschutzbeauftragter](#)“, [Kennzahl 2356](#)

3. Rechtsgrundlage und Zweck der Datenverarbeitung (Art. 6 DSGVO)

Es ist anzugeben, auf **welcher Rechtsgrundlage** und für **welche Zwecke**, die personenbezogenen Daten verarbeitet werden sollen. Die häufigsten Rechtsgrundlagen für eine Datenerhebung dürfte der Vertrag, eine Einwilligung oder das sich ergebende berechnete Interesse des Datenerhebers sein. Zweck kann z.B. sein: die Verarbeitung und Weiterleitung der Kundenadresse an den Paketversender im Onlineshop oder der Einsatz von Google Analytics.

Der Betroffene ist darüber zu informieren, ob er gesetzlich oder vertraglich zur Bereitstellung der personenbezogenen Daten verpflichtet ist oder ob dies für einen Vertragsabschluss erforderlich ist. Zudem muss darüber belehrt werden, welche möglichen Folgen die Nichtbereitstellung hat.

a) Vertrag

Die Verarbeitung personenbezogener Daten kann zur **Erfüllung eines Vertrags** oder zur Durchführung **vorvertraglicher Maßnahmen**, die auf Anfrage der betroffenen Person erfolgen, erforderlich sein (Art. 6 Abs. 1 lit. b DSGVO). Angaben wie der Name des Kunden oder seine Adresse sind z. B. nötig, um im Rahmen eines Kaufvertrages die Ware zu liefern.

***Wichtig:** Liegt ein Vertrag vor, muss nicht noch zusätzlich eine Einwilligung eingeholt werden. Denn: Verträge haben für die Dauer ihrer Laufzeit Bestand, Einwilligungen können jederzeit widerrufen werden.*

b) Einwilligung

Eine Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) ist insbesondere beim Versand von Newslettern oder beim Setzen nicht erforderlicher Cookies notwendig. Die Voraussetzungen einer wirksamen Einwilligung sind in Art. 7, 8 DSGVO festgelegt. Sie muss **freiwillig für den bestimmten Fall, in informierter Weise** und **unmissverständlich** abgegeben worden sein. Sie ist zu dokumentieren. Der Betroffene ist auf die Möglichkeit hinzuweisen, dass er jederzeit die Einwilligung **mit Wirkung für die Zukunft widerrufen** kann.

→ D02 „[Einwilligung nach der DSGVO](#)“, [Kennzahl 2356](#)

c) Berechnete Interessen

Ein berechnetes Interesse kommt nur dann in Betracht, wenn weder ein Vertrag noch eine Einwilligung vorliegt. Bei einem berechneten Interesse ist abzuwägen, ob derjenige, dessen personenbezogenen Daten erhoben werden, weniger schutzwürdig ist als der Unternehmer, der diese Daten erhebt. Es muss im Rahmen der Datenschutzerklärung angegeben werden, wie diese Abwägung aussieht. Dies ist beispielsweise der Fall bei einem Kontaktformular, das der Kunde im Online-Shop ausfüllt. Der Online-Händler hat ein berechnetes Interesse an dessen Mail-Adresse, um dem Kunden die angeforderten Informationen geben zu können.

4. Empfänger der Daten

Ist eine Übermittlung personenbezogener Daten an Dritte beabsichtigt, ist der **Empfänger** anzugeben. Steht noch nicht fest, wer die Daten empfangen soll, reichen auch Angaben zur **Kategorie der Empfänger**, etwa „Weitergabe an Werbepartner“, „Weitergabe an Versandunternehmen“.

5. Datentransfer in Drittstaaten

Werden Daten in einen Staat außerhalb der EU oder an eine internationale Organisation übertragen, ist darüber stets zu informieren. Bei der Übermittlung personenbezogener Daten in ein Nicht-EU-Land sind zusätzliche Garantien notwendig, die ein angemessenes Datenschutzniveau im Drittland gewährleisten. Zu diesen Garantien gehören beispielweise die [EU-Standardvertragsklauseln](#). Für den Datenaustausch mit den USA hat die EU-Kommission einen Angemessenheitsbeschluss für das sog. EU-U.S. Data Privacy Framework erlassen. Ähnlich wie beim vorausgegangenen Privacy Shield können sich Unternehmen zertifizieren und auf eine Liste aufnehmen lassen.

6. Dauer der Speicherung bzw. Kriterien für die Festlegung der Dauer

Das Unternehmen muss angeben, wie lange es die Daten speichert. Dabei ist der Grundsatz der **Datenminimierung** zu beachten: Werden die Daten nicht mehr benötigt, sind sie zu löschen. Zu beachten sind dabei immer die handels- und steuerrechtlichen Aufbewahrungsfristen.

7. Betroffenenrechte

Der Betroffene ist darüber aufzuklären, dass ihm ein Recht auf **Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch** und das **Recht auf Datenübertragbarkeit** zusteht.

8. Beschwerderecht bei der Aufsichtsbehörde

Der Betroffene hat jederzeit das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn er sich in seinen Rechten nach der DSGVO verletzt sieht. Die Beschwerde kann insbesondere bei der Aufsichtsbehörde eingelegt werden, in deren Mitgliedstaat er seinen gewöhnlichen Aufenthalt hat. Die Adresse der zuständigen Aufsichtsbehörde ist im Rahmen der Datenschutzerklärung anzugeben. Die Aufsichtsbehörden sind verpflichtet, Maßnahmen zur Erleichterung der Einreichung von Beschwerden zu treffen, wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

9. Profiling

Beim Profiling oder einer anderen automatisierten Entscheidungsfindung sind aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zur Verfügung zu stellen.

10. Herkunft der Daten

Werden die Daten bei jemand anderen als dem Betroffenen erhoben, muss die Quelle offengelegt werden, von der die Daten stammen. Dies gilt auch, wenn die Daten aus einer öffentlich zugänglichen Quelle stammen.

11. Bereitstellung der Webseite

Auf der Unternehmenswebseite werden in der Regel personenbezogene Daten durch Drittanbieter oder durch eigene Funktionen erhoben. Auch hierüber muss informiert werden.

Am 1. Dezember 2021 ist zudem das Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) in Kraft getreten, in dem weitere Pflichten für Telemedienanbieter wie z.B. Webseiten-Anbieter festgelegt sind. So sind technische und organisatorische Vorkehrungen zu treffen, um

- den Schutz der Nutzer gegen Kenntnisnahme Dritter sicherzustellen,
- die Möglichkeit zu bieten, einen genutzten Dienst jederzeit beenden zu können,
- die Möglichkeit einer anonymisierten oder pseudonymisierten Dienstenutzung zu bieten, soweit dies technisch möglich und zumutbar ist und
- die Weiterleitung zu einem anderen Telemedienanbieter anzuzeigen.

Darüber hinaus können über folgende technischen Einrichtungen Nutzerdaten erhoben werden, über die informiert werden muss:

a) Log-Dateien

Log-Dateien protokollieren die Aktivitäten der Seitenbesucher. Dadurch können unter anderem Fehler aufgespürt und beseitigt werden. Die Log-Dateien speichern unter anderem folgende personenbezogene Daten:

- Uhrzeit zum Zeitpunkt des Seitenzugriffs
- URL der besuchten Website
- Menge der übertragenen Daten in Byte
- Information über die Quelle, über die Besucher auf die Seite gelangen
- Angabe des Browsertyps
- Information zum Betriebssystem
- IP-Adresse des Besuchers

Rechtsgrundlage für die Verarbeitung dieser Daten ist Art. 6 Abs. 1 lit. f DSGVO. Berechtigte Interessen können die statistische Auswertung der Seitenbesuche, sowie die Sicherheit und Funktionsfähigkeit der Website sein.

b) Cookies

Cookies sind kleine Textdateien, die auf dem Rechner des Besuchers abgelegt werden, um das Angebot auf seine Bedürfnisse abzustimmen und ihm die Nutzung bestimmter Funktionen zu ermöglichen. Auch mithilfe Cookies werden personenbezogene Daten erhoben, da Rückschlüsse auf eine natürliche Person möglich sind. Mit permanenten Cookies können wiederkehrende Besucher auf der Seite erkannt werden. Wenn Cookies verwendet werden, muss der **Kunde im Rahmen der Datenschutzerklärung darauf hingewiesen** werden, dass es sich um **Nutzungsdaten** handelt. Er ist auch darüber zu informieren, dass er durch **Einstellung seines Browsers** das Abspeichern von Cookies verhindern kann, dadurch jedoch eventuell bestimmte Funktionen der Internetseite nicht mehr genutzt werden können.

Für die Verwendung von Cookies bedarf es deshalb ebenfalls einer Rechtsgrundlage. Nach Ansicht des EuGH (Urt. v. 1.10.2019, C-673/17) dürfen **nicht erforderliche Cookies nur mit einer aktiven Einwilligung** gesetzt werden. Irrelevant ist, ob es sich bei den im Endgerät des Nutzers einer Website gespeicherten oder abgerufenen Informationen um personenbezogene Daten handelt oder nicht.

§ 25 TTDSG regelt die Voraussetzungen für das Setzen von Cookies. Danach ist die Speicherung von Cookies auf dem Endgerät nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen **eingewilligt** hat. Eine Einwilligung ist nicht notwendig, wenn die Speicherung unbedingt erforderlich ist, damit der Anbieter des Telemediendienstes den „vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann“. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden (DSK) stellen dazu eine [Orientierungshilfe](#) bereit.

Beispiele für notwendige Cookies: *Session-Cookies (Warenkorb, User-Input), Authentifizierungs-Cookies, Cookies zur Anpassung der Benutzeroberfläche, Sicherheits-Cookies*

Beispiele für nicht notwendige Cookies: *Tracking-Cookies, Cookies zur Reichweitenmessung und Websitenoptimierung; Cookies zur Einbindung von Drittinhalten oder Drittdiensten*

c) Analyse-/Marketing-Tools

Mit Hilfe von Analyse-Tools, wie z.B. Google Analytics oder Matomo, kann die Art und Zahl der Zugriffe und Nutzung der Seite ausgewertet werden, um so das Angebot zu optimieren. Da derartige Tools u.a. IP-Adressen (= personenbezogene Daten) erheben, verarbeiten und speichern, muss der Besucher über die Datenverarbeitung und -übermittlung aufgeklärt werden.

Nach § 25 TTDSG ist zudem eine **Einwilligung** notwendig. Darüber hinaus müssen die Analyse-Tools so eingerichtet sein, dass die **IP-Adressen anonymisiert** übermittelt werden. Mit Google ist ein **Auftragsverarbeitungs-**Vertrag abzuschließen.

d) Social-Plugins sozialer Netzwerke

Viele Webseitenbetreiber verwenden Plugins sozialer Netzwerk wie Facebook, u.ä., die z.B. in Form eines „Gefällt mir“ auf der Seite installiert werden können. Problematisch an diesen Plugins ist, dass bereits mit Aufruf der Internetseite eine Verbindung mit den Servern des jeweiligen Netzwerks hergestellt und die IP-Adresse des Besuchers übermittelt wird. Dies gilt unabhängig davon, ob die Person bei dem sozialen Netzwerk eingeloggt bzw. registriert ist.

Nach Ansicht des Landgericht Düsseldorf (Urteil vom 09.03.2016, Az.: 12 O 151/15) sind solche Plugins wettbewerbswidrig. Der EuGH hat entschieden (Urteil vom 29.07.2019, C-40/17, Celex-Nr. 62017CJ0040 - „Fashion ID“), dass der Webseitenanbieter gemeinsam mit dem Anbieter des Social Plugins mitverantwortlich für die Datenverarbeitung ist.

Ratsam ist es, lediglich auf den Social Media-Auftritt **zu verlinken**. In diesem Fall ist darauf hinzuweisen, dass der Link zur Webseite eines Drittanbieters führt. Alternativ sollte auf die sog. **2-Klick oder Shariff-Lösung** zurückgegriffen werden. Dabei wird das Plugin zunächst nur als bloße Grafik ohne aktive Funktion auf der Seite angezeigt. Erst durch Anklicken wird dann das eigentliche Plugin aktiviert und die Verbindung zu den Servern hergestellt. Auf diese Weise muss der Besucher aktiv einwilligen, bevor seine Daten an das Netzwerk weitergeleitet werden. Auch darüber muss in der Datenschutzerklärung informiert werden.

e) Newsletter/Newsletter-Tracking

Viele Unternehmer verschicken Newsletter zu Werbezwecken. Rechtsgrundlage für das Versenden des Newsletters ist die Einwilligung des Betroffenen nach Art. 6 Abs. 1 lit. a DSGVO. Die Einwilligung wird im Rahmen des Anmeldevorgangs durch die sog. **Double-Opt-In-Methode** eingeholt. Dabei meldet sich der Kunde mit seiner E-Mail-Adresse an. Das Unternehmen verschickt daraufhin eine Bestätigungs-Mail mit einem Anmelde-link. Durch Aktivieren des Links gibt der Kunde seine Einwilligung zum Versand von Newslettern. Setzt die Webseite ein **Newsletter-Tracking** ein, ist hierfür ebenfalls eine Einwilligung notwendig.

f) Kontaktformular

Unternehmen bieten Ihren Kunden in der Regel an, durch ein Formular mit dem Unternehmen in Kontakt zu treten. Dabei werden personenbezogene Daten gespeichert. Rechtsgrundlage dafür ist die Einwilligung des Kunden nach Art. 6 Abs. 1 lit. a DSGVO. Zielt der Kontakt zum Abschluss eines Vertrages ab, so ist Rechtsgrundlage für die Verarbeitung Art. 6 Abs. 1 lit. b DSGVO. Im Kontaktformular sollten nur notwendige Angaben abgefragt werden. Die Daten dürfen nur solange gespeichert werden, wie dies für die Bearbeitung der Anfrage notwendig ist.

Die Übermittlung des Kontaktformulars muss über eine **verschlüsselte Verbindung** (SSL-Protokoll) erfolgen.

g) Registrierung auf der Webseite

Besteht auf der Internetseite die Möglichkeit, sich unter Angabe personenbezogener Daten zu registrieren, muss der Kunde darüber informiert werden, was mit seinen angegebenen Daten passiert. Rechtsgrundlage für die Verarbeitung ist die Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO. Dient die Registrierung zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen, so ist Art. 6 Abs. 1 lit. b DSGVO Rechtsgrundlage. Entsprechend ist im Rahmen der Datenschutzerklärung zu informieren.

Achtung: Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat beschlossen, dass Onlinehändler grundsätzlich einen [Gastzugang](#) anbieten müssen.

h) Eingebundene Videos von YouTube & Vimeo

Werden auf der Webseite Videos eingebunden, wird ebenfalls bereits beim Laden der Seite die IP-Adresse des Seitenbesuchers gespeichert. Die Speicherung erfolgt unabhängig davon, ob der Besucher das Video anklickt oder nicht.

Bei einer Verlinkung auf die Video-Plattform ist darüber zu informieren, dass der Link zu einer Webseite eines Drittanbieters führt.

Wird der Dienst direkt auf der Seite eingebunden, erfolgt regelmäßig eine Übermittlung von personenbezogenen Daten an Drittanbieter. In diesem Fall ist zusätzlich eine Einwilligung erforderlich. Die Videos sollten im erweiterten Datenschutzmodus eingebettet werden. Alternativ kann auf die 2-Klick oder Shariff-Lösung zurückgegriffen werden.

i) Externe Schriften und Dateien wie z. B. Google Fonts

Auf Internetseiten werden neben den Standardschriften in der Regel auch Schriftarten von anderen Anbietern benutzt. Bei der Verwendung externer Schriftarten wie z.B. Google Fonts, werden diese üblicherweise beim Laden der Seite von den Servern des Anbieters nachgeladen. Dabei findet ein Datenaustausch zwischen der Website und dem externen Anbieter statt.

Um die Schriften und Dateien zu nutzen und den Regeln der DSGVO zu entsprechen, sollten Sie den Datenaustausch mit externen Servern unterbinden, indem Sie die Schriften herunterladen und anschließend die Daten **lokal in Ihrem Webspacespeichern** und von dort verwenden.

j) Bezahldienste

Bedient sich der Unternehmer zur Abwicklung Bezahldienste Dritter oder Payment-Verfahren, werden die Daten an Dritte weitergegeben. Auch darüber muss der Kunde im Rahmen der Datenschutzerklärung informiert werden.

Dieses Merkblatt soll – als Service Ihrer IHK – nur erste Hinweise geben und erhebt daher keinen Anspruch auf Vollständigkeit. Obwohl es mit größtmöglicher Sorgfalt erstellt wurde, kann eine Haftung für die inhaltliche Richtigkeit nicht übernommen werden.