DATENSCHUTZ – D07

Stand: Oktober 2018

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

Webseitenbetreiber und auch andere Unternehmen hatten bislang die Verpflichtung, allgemein über Art, Umfang und Zweck der Erhebung und Verwendung der personenbezogenen Daten zu unterrichten. Dies geschah im Rahmen der Datenschutzerklärung. Der **Umfang der Informationspflichten** wird durch die DSGVO **erweitert.** Nach dem Wortlaut von Art. 13 Abs. 1 DSGVO sollen diese **Informationen zum Zeitpunkt der Erhebung der Daten** gegeben werden. Dies ist beim stationären Einzelhandel machbar, wenn in Anwesenheit des Kunden die Vertragsdaten aufgenommen werden. Beim Onlinehandel scheidet das dagegen aus. Die Lösung: Das Unternehmen hält eine **generelle Datenschutzerklärung** vor, die an zentraler Stelle jederzeit eingesehen werden kann und über alle datenschutzrelevanten Umstände informiert. Dies kann auf der Unternehmens-Homepage erfolgen oder über ein Infoblatt, das im Ladengeschäft bereitgehalten wird.

Wichtig: *Hält der Unternehmer eine Datenschutzerklärung vor, die DSGVO-konform ist, ist er nicht mehr verpflichtet, vor jeder Datenerhebung eine Belehrung nach Art. 13, 14 DSGVO durchzuführen.*

➔**D05** „Informationspflichten nach der DSGVO“, **Kennzahl 2158**

Hinweis: Jeder Unternehmer, der eine eigene Internetseite betreibt oder auf Plattformen vertreten ist, muss eine Datenschutzerklärung bereit halten, da personenbezogene Daten erhoben werden. 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

Die Datenschutzerklärung ist in **präziser, transparenter, verständlicher** und **leicht zugänglicher Form** in einer **klaren und einfachen Sprache** zur Verfügung zu stellen. Die Informationen sind **schriftlich** oder in anderer Form, gegebenenfalls auch **elektronisch**, bereitzuhalten.

Industrie- und Handelskammer des Saarlandes
Postanschrift: IHK Saarland │ 66104 Saarbrücken │ Büroanschrift: Franz-Josef-Röder-Straße 9 │ 66119 Saarbrücken
Tel. 0681/9520-0 │ Fax 0681/9520-888 │ E-Mail: info@saarland.ihk.de │ Internet: www.saarland.ihk.de

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 „Datenschutzinformationen“. Nicht ausreichend ist das „Verstecken“ in den AGB. Die konkrete Ausgestaltung der Datenschutzerklärung hängt im Wesentlichen davon ab, welche Daten erhoben werden.

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.

Wird die **Datenschutzerklärung** auf die **Unternehmens-Homepage** eingestellt, 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**

Inhalt der Datenschutzerklärung

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

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.

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 2158**

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

Neu ist die **verpflichtende Angabe der Rechtsgrundlage** für die Verarbeitung und die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen. Die häufigsten Rechtsgrundlagen in der Wirtschaft für eine Datenerhebung dürfte der Vertrag, eine einzuholende Einwilligung oder das sich ergebende berechtigte Interesse des Datenerhebers sein. Unter die Erklärung des Zwecks fällt etwa 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. 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

Die Verarbeitung personenbezogener Daten ist zulässig, wenn sie auf einer Einwilligung beruht, Art. 6 Abs. 1 lit. a DSGVO. Eine Einwilligung ist insbesondere beim Versand von Newsletter 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.

c) Berechtigte Interessen

Eine völlig neue Rechtsgrundlage wurde mit der DSGVO eingeführt: Das berechtigte Interesse nach Artikel 6 Abs. 1 lit. f DSGVO. Ein berechtigtes Interesse kommt nur dann in Betracht, wenn weder ein Vertrag noch eine Einwilligung vorliegt. Bei einem berechtigten 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 berechtigtes 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 stets zu informieren. Dabei ist auch die Rechtsgrundlage zu nennen, auf die sich der Unternehmer beruft.

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.

➔**D05** „Informationspflichten nach der DSGVO", **Kennzahl 2158**

8. Widerruf der Einwilligung

Beruht die Verarbeitung auf einer Einwilligung des Betroffenen, muss er darauf hingewiesen werden, dass er die Einwilligung jederzeit **für die Zukunft widerrufen** kann.

9. Bestehendes 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.

10. Bereitstellung der Webseite

Auf der Unternehmenswebseite werden in der Regel personenbezogene Daten durch Drittanbieter oder durch eigene Funktionen erhoben. Über folgende technischen Einrichtungen können Nutzerdaten erhoben werden:

a) Log-Dateien

Log-Dateien protokollieren die Aktivitäten der Seitenbesucher. Dadurch können unter anderem Fehler aufgespürt und beseitigt werden. Die Log-Dateien speichern unter anderen folgenden personenbezogenen 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 Browserstyps
- 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. Für die Verwendung von Cookies bedarf es deshalb ebenfalls einer Rechtsgrundlage. Die Einholung einer Einwilligung vor der Verarbeitung erscheint wenig sinnvoll. Nach überwiegender Ansicht ist Art. 6 Abs. 1 lit. f DSGVO die Rechtsgrundlage für die Verwendung von Cookies. Eine abschließende Klärung steht noch aus.

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.

c) Analyse-Tools

Mit Hilfe von Analyse-Tools, wie z.B. Google Analytics, Matomo (früher: Piwik) oder ähnlichen, kann die Art und Zahl der Zugriffe und Nutzung der Seite ausgewertet werden, um so das Angebot zu optimieren. Da derartige Tracking-Tools u.a. IP-Adressen (= personenbezogene Daten) erheben, verarbeiten und speichern, muss der Besucher darüber aufgeklärt werden. Auch hier könnte als Rechtsgrundlage Art. 6 Abs. 1 lit. f DSGVO herangezogen werden. Klarheit soll die neue ePrivacy-Verordnung bringen. Auch hierüber muss **im Rahmen der Datenschutzerklärung** informiert werden. Als berechtigtes Interesse im Sinne von Art. 6 Abs. 1 lit. f DSGVO können etwa wirtschaftliche Interessen angegeben werden.

Wichtig ist die Einbindung eines Opt-Out-iFrames, damit Besucher der Internetseite das Tracken deaktivieren können. Darüber hinaus müssen die Analyse-Tools so eingerichtet sein, dass die IP-Adressen anonymisiert übermittelt werden. Mit Google ist ein AV-Vertrag abzuschließen.

➔**D12** „Auftragsverarbeitung nach der DSGVO“, **Kennzahl 2158**

d) Social-Plugins sozialer Netzwerke

Viele Webseitenbetreiber verwenden Plugins sozialer Netzwerk wie Facebook, Google+ 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 Düsseldorfs (Urteil vom 09.03.2016, Az.: 12 O 151/15) sind solche Plugins wettbewerbswidrig. Ratsam ist es, das Plugin zunächst nur als bloße Grafik ohne aktive Funktion auf der Seite anzuzeigen. 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 (sog. 2-Klick oder Shariff-Lösung). Auch darüber muss informiert werden.

Rechtsgrundlage für die Verwendung von Social Plugins ist Art. 6 Abs. 1 lit. f DSGVO.

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 Anmeldelink. Durch Aktivieren des Links gibt der Kunde seine Einwilligung zum Versand von Newslettern.

Setzt die Webseite ein **Newsletter-Tracking** ein, ist darauf ebenfalls einzugehen. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO.

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. Die Daten dürfen nur solange gespeichert werden, wie dies für die Bearbeitung der Anfrage notwendig ist.

Die Übermittlung des Kontaktformulars sollte über eine angemessene 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 angegeben 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.

h) 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 Webspace speichern und von dort verwenden. Als Rechtsgrundlage ist im Rahmen der Datenschutzerklärung anzugeben Artikel 6 Abs. 1 lit. f DSGVO.

i) 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.

11. 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.

12. 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.