



Datenschutz im Internet – Die Datenschutzerklärung

I. Grundsätzliches zu Informationspflichten bei Angeboten im Internet

Bietet jemand einen elektronischen Informations- oder Kommunikationsdienst an, gelten besondere Informationspflichten in Bezug auf eine damit verbundene Verarbeitung personenbezogener Daten. Zu solchen Diensten zählen etwa eine Webseite mit unmittelbar abrufbarem oder bestellbarem Angeboten wie Online-Shops, Presse- oder Wetterseiten, aber auch Webseiten mit Kontaktformular oder Kommentarfunktion, Apps, Werbemails oder Social Media.

Diesen Informationspflichten sollte im Rahmen einer Datenschutzerklärung nachgekommen werden.

Derzeit ergeben sich die hiermit verbundenen Informationspflichten noch aus dem Telemediengesetz (TMG). Mit Geltung der Datenschutzgrundverordnung (DS-GVO) ab dem 25. Mai 2018, wird sich dies auch noch nicht maßgeblich ändern. Die DS-GVO regelt die Pflichten der Diensteanbieter nicht spezifisch für Informations- und Kommunikationsdienste, da sich derzeit eine weitere Europäische Verordnung im Entstehungsprozess befindet, die sogenannte ePrivacy-Verordnung, die dann für diesen spezifischen Bereich gelten wird. Bis zum Inkrafttreten der ePrivacy-Verordnung (Zeitpunkt derzeit nicht absehbar, möglicherweise aber noch 2019), werden ab Ende Mai 2018 das TMG, sowie die allgemeinen Regeln aus der DS-GVO nebeneinander gelten.

Für Diensteanbieter relevant dürften ergänzend zu den bereits bestehenden Pflichtangaben nach dem TMG vor allem die Informationspflichten aus Art. 12 bis Art. 14 DS-GVO sein. Wie im Rahmen von § 13 TMG, gilt es auch hiernach, Informationen zu Art, Umfang und Zweck der Verarbeitung personenbezogener Daten bereitzustellen, ebenso wie Kontaktdaten und Anschrift des jeweiligen Diensteanbieters. Eine wesentliche Neuerung durch die DS-GVO wird sein, dass der Diensteanbieter auch über die Rechtsgrundlage informieren muss, auf die er die Datenverarbeitung stützt – also entweder einen näher benannten gesetzlichen Erlaubnistatbestand, oder eine Einwilligung, auf deren Widerruflichkeit der Diensteanbieter ebenfalls hinzuweisen hat.

II. Art und Weise der Information

Auf die Datenschutzerklärung sollte mittels eines sprechenden Links auf **jeder** Seite Bezug genommen werden. Alternativ kann auch eine eigenständige Kundeninformationsseite eingerichtet werden. Aber auch diesbezüglich bedarf es eines ausdrücklichen Links, der stets für den Betroffenen verfügbar und zugänglich ist. Unzureichend ist ein Link auf AGB, in denen sich datenschutzrechtliche Regelungen enthalten. Die Datenschutzerklärung ist eine einseitige Erklärung der datenverarbeitenden Stelle. Es handelt sich hierbei nicht um AGB, da durch die Datenschutzerklärung nichts vereinbart wird. In eine Datenschutzerklärung muss der Kunde oder Nutzer daher auch nicht einwilligen. Er kann auch der Geltung nicht zustimmen.

III. Die Datenschutzerklärung im Einzelnen

Die inhaltliche Ausgestaltung einer solchen Datenschutzerklärung richtet sich danach, welche Funktionen der jeweilige Dienst vorsieht und welche Daten hierbei auf welche Weise verarbeitet werden. Daraus ergibt sich, dass es eine Musterdatenschutzerklärung nicht geben kann, da dies stets nur für den jeweiligen Einzelfall ausgedrückt werden kann. Als Checkliste – mehr aber auch nicht – kann der [„One-Pager“ und dessen Erläuterungen des Bundesministeriums der Justiz und für Verbraucherschutz](#) dienen.

Eine Mustergliederung mit entsprechenden Pflichtangaben nach der DS-GVO und was die Hinweise im Einzelnen umfassen sollten findet sich zudem [hier](#).

Aus der DS-GVO ergibt sich, dass die Datenschutzerklärung in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache über eine Reihe an Informationen bezogen auf die Art, den Umfang und den Zweck jeder Verarbeitung von personenbezogenen Daten informieren muss. Aus § 13 TMG und Art. 13 DS-GVO ergeben sich folgende Pflichtangaben:

1. Name und Kontaktdaten (Anschrift, E-Mail-Adresse, ggf. Telefon und Fax) des Diensteanbieters und ggf. dessen Vertreters,
2. Kontaktdaten des Datenschutzbeauftragten, falls Bestellungspflicht besteht (Weitere Informationen hierzu finden Sie in unserem Merkblatt [„Der betriebliche Datenschutzbeauftragte“](#)),
3. alle Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen,
4. die jeweilige Rechtsgrundlage für die Verarbeitung (Einwilligung oder gesetzlicher Erlaubnistatbestand), (unterschiedliche Zwecke benötigen ggf. einen eigenständigen Erlaubnistatbestand),
5. ggf. die berechtigten Interessen zur Datenverarbeitung, sofern diese auf eine Interessenabwägung nach Art. 6 Abs. 1 lit. f) DS-GVO gestützt wird,
6. bei Weitergabe von personenbezogenen Daten die Empfänger oder Kategorien von Empfängern,
7. ggf. die Absicht des Diensteanbieters, personenbezogene Daten an ein Drittland (z. B. USA) zu übermitteln, sowie damit verbundene weitere spezifische Pflichtinformationen,
8. die Dauer, für die die personenbezogenen Daten gespeichert werden bzw. Kriterien, anhand derer diese ermittelt werden soll,



9. das Bestehen der speziellen Rechte der Betroffenen aus der DS-GVO, also Auskunftsrecht (Art. 15 DSGVO), Lösch- und Berichtigungsanspruch (Art. 16 u. 17 DSGVO), Einschränkung der Verarbeitung (Art. 18 DSGVO), Widerspruchsrechts (Art. 21 DSGVO), Recht auf Datenübertragbarkeit (Art. 20 DSGVO),
10. bei Verarbeitung aufgrund Einwilligung auf das Recht, die Einwilligung jederzeit zu widerrufen,
11. Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde und bei welcher,
12. ob Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte,
13. sofern Zweckänderung der Datenverarbeitung erfolgen soll, Informationen hierüber,
14. Des Weiteren muss die Datenschutzerklärung einen Hinweis auf eine anonyme/pseudonyme Nutzungsmöglichkeit der Website hinweisen, soweit eine solche besteht.
15. Sollen Daten zu Werbezwecken genutzt werden, muss die Datenschutzerklärung einen Hinweis zu den bestehenden Widerspruchs- oder Widerrufsmöglichkeiten gegen eine solche Nutzung der Daten enthalten (vgl. nachstehende Ziffer V).
16. Da der Inhalt der innerhalb des Dienstes erteilbaren Einwilligungen jederzeit abrufbar sein muss, sollten diese in der Datenschutzerklärung wiederholt werden.
17. Sollte die Website eine Bonitätsprüfung vornehmen, ist dringend zu empfehlen, diese ebenfalls nur im Falle einer ausdrücklich erklärten Einwilligung vorzunehmen. Zwar genügt bei einem berechtigten Interesse (Bsp.: Online-Händler tritt in Vorleistung) – aber auch nur dann – der Hinweis auf eine Abbruchmöglichkeit, allerdings besteht auch in diesem Fall eine gewisse Rechtsunsicherheit, sodass die Annahme eines solchen Interesses mit Vorsicht zu erfolgen hat. Zudem ist es von Vorteil, den Datenempfänger genau zu bezeichnen. Zu berücksichtigen gilt es auch, dass die Bonitätsprüfung in der Regel auch Score-Werte enthält. Dann ist mitzuteilen, auf welcher wissenschaftlichen Grundlage das Prüfungsverfahren erfolgt.
18. Sollten Daten außerhalb der Vertragserfüllung an Dritte weitergegeben werden, so sind dem Betroffenen der Empfänger und der Zweck der Weitergabe in der Datenschutzerklärung zu nennen.
19. Gegebenenfalls hat ein Hinweis auf eine verschlüsselte Datenübertragung zu erfolgen.

20. Werden Tracking-Tools, Social-Media Plug-Ins, Cookies und ähnliches eingesetzt, muss hierauf ebenfalls hingewiesen und der konkret verwendete Dienst benannt werden. Wenn diese Dienste zu einer Datenübermittlung in ein Drittland (z.B. USA) führen, gelten die oben genannten zusätzlichen besonderen Anforderungen und Informationspflichten.

III. Rechtliche Folgen und Hintergründe

Hintergrund dieser zahlreichen Informationspflichten ist es, dass der Gesetzgeber an die Verarbeitung sogenannter personenbezogener Daten hohe Anforderungen stellt, da diese einen schwerwiegenden Eingriff in die Privatsphäre einer jeden Person darstellen kann. Daher soll es nicht jedem gestattet sein, jedermanns personenbezogene Daten nach Belieben zu verwenden.

1. Der Begriff der personenbezogenen Daten

Aus diesem Grund knüpfen sowohl § 13 TMG, der die Pflichten des Diensteanbieters regelt, als auch die DS-GVO knüpfen an die Verarbeitung personenbezogener Daten an.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche 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 (Art. 4 Nr. 1 DS-GVO).

Umfasst sind danach etwa der Name, Adressangaben einschließlich E-Mail-Adresse und Telefonnummer, Geburtsdatum und Kontonummer, aber auch die ungekürzte IP-Adresse. Auch bei Verwendung von Social-Media-Plug-Ins wie den Facebook-„Like“-Button oder Cookies werden daher unter Umständen personenbezogene Daten verarbeitet. Somit ist auch auf eine nicht sichtbare, automatisierte Datenerhebung hinzuweisen, wie sie etwa durch Web-Analyse-Tools durchgeführt wird. In diesem Fall gelten zudem weitergehende Voraussetzungen, da innerhalb der Webanalysedienste eine Profilbildung stattfindet. Insoweit ist ein ausdrückliches Einverständnis dahingehend erforderlich, dass eine Verknüpfung zwischen diesem Profil und personenbezogenen Daten erfolgt. Hinsichtlich eines solchen Einverständnisses muss eine ständige Widerrufsmöglichkeit gegeben sein, auf die entsprechend hinzuweisen ist.

2. Erlaubnis der Datenverarbeitung – Gesetz und Einwilligung

Nach dem im Datenschutz geltenden Zweckbindungsgrundsatz, ist jede Datenerhebung nur zu einem vorher bestimmten Zweck erlaubt und muss durch ein Gesetz oder eine Einwilligung legitimiert sein. Im Falle einer gesetzlichen Erlaubnis bedarf es keiner ausdrücklichen Einwilligung des Betroffenen. Beispiel für eine gesetzliche Erlaubnis ist § 28 Abs. 1 Nr. 1 BDSG a.F., bzw. Art. 6 Abs. 1 lit. b) DS-GVO, wonach es zulässig ist, Daten zur Erfüllung eines Vertrages weiterzugeben – wie etwa die Übermittlung der Adressdaten des Kunden an das ausliefernde Transportunternehmen im Rahmen eines Kaufvertrages.



Ansonsten ist grundsätzlich jegliche Art der Datenverarbeitung möglich, soweit der Betroffene ausdrücklich und freiwillig eingewilligt hat. An die Freiwilligkeit der Einwilligung stellt die DS-GVO besondere Ansprüche. So enthält etwa Art. 7 Abs. 4 DS-GVO ein sog. Kopplungsverbot. Danach kommt es bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde auch darauf an, ob unter anderem die Erfüllung eines Vertrags von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind. Es kann also keine wirksame Einwilligung eingeholt werden, wenn der Betroffene in die Verarbeitung von Daten einwilligen muss, die für die Erfüllung eines zugrundeliegenden Vertrages überhaupt nicht erforderlich wären.

Eine ausdrückliche Einwilligung liegt nicht vor, wenn diese in AGB oder mittels einer vorangekreuzten Erklärung erfolgt. Zudem muss die Erklärung den Zweck der Verarbeitung benennen. Diese Einwilligung muss für den Betroffenen jederzeit abrufbar sein. Zudem kann sie jederzeit widerrufen werden, mit der Folge, dass die Zulässigkeit der weiteren Datenverarbeitung endet.

In jedem Fall dürfen immer nur so wenige Daten wie möglich erhoben werden (sog. Grundsatz der Datenminimierung). Zudem muss bei der Datenerhebung beim Betroffenen gekennzeichnet werden, ob es sich um Pflichtangaben oder freiwillige Angaben handelt, sodass der Betroffene selbst entscheiden kann, ob er diese tätigt oder nicht.

Wichtige Grundprinzipien der DS-GVO im Zusammenhang mit Datenschutz im Internet sind zudem das Konzept des Datenschutzes durch Technik (sog. „Privacy by Design“) und datenschutzfreundlicher Voreinstellungen (sog. „Privacy by Default“) (Art. 25 DS-GVO). Privacy by Design meint, dass der Diensteanbieter sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen. Durch Privacy by Default wird sichergestellt, dass technische Voreinstellungen immer so zu erfolgen haben, dass ohne Eingreifen der betroffenen Person nur die für den jeweiligen Zweck erforderlichen Daten verarbeitet und Dritten zugänglich gemacht werden können.

IV. Sonderfall Cookies

Im Zusammenhang mit der Verwendung von Cookies, sofern sie personenbezogene Daten speichern, besteht die Besonderheit, dass die Situation in besonderem Maße durch eine unklare Rechtslage geprägt ist. Hintergrund ist die streitige Frage, ob die bestehende nationale gesetzliche Regelung des § 13 TMG bereits für die Umsetzung der unionsrechtlichen Cookie-Richtlinie ausreicht. Insoweit ist bisher nicht geklärt, wie den datenschutzrechtlichen Bestimmungen in Bezug auf Cookies entsprochen werden kann, ob eine ausdrückliche Einwilligung in Form eines Opt-In erforderlich ist, oder ein Opt-Out, also die Widerspruchsmöglichkeit, ausreicht. Auch die DS-GVO kann hier keine Klärung schaffen. Stattdessen ist nun nicht einmal mehr klar, ob und inwiefern die DS-GVO den Einsatz von Cookies regelt. Klarheit kann hier wohl nur die noch im Entwurf befindliche ePrivacy-Verordnung schaffen, da der Einsatz von Cookies unter deren Regelungsrahmen fallen dürfte.



Vorerst wird es wohl der Sache nach bei der derzeitigen Rechtslage bleiben:

Bei dem Einsatz von Cookies, die eine spätere Identifizierung des Nutzers ermöglichen (zum Beispiel Cookies, die die Speicherung der Log-In-Daten für einen späteren Besuch der Website ermöglichen), ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Diese Unterrichtung hat jederzeit abrufbar zu sein. Außerdem sind Angaben erforderlich, die die Möglichkeit der Ablehnung von Cookies beinhalten. Zur Erfüllung dieser Vorgaben wird eine Lösung mittels Bannern empfohlen, die sich mittlerweile in der Praxis auch weitestgehend durchgesetzt hat.

In der Datenschutzerklärung muss zudem darüber informiert werden, welchem Verwendungszweck die Cookies dienen und dass es über den Browser die Möglichkeit gibt bestimmte oder auch alle Cookies abzulehnen. Geht man von der Anwendbarkeit der DS-GVO aus, muss in der Datenschutzverordnung zudem darauf hingewiesen werden, aufgrund welcher Rechtsgrundlage die Verarbeitung personenbezogener Daten bei der Verwendung von Cookies erfolgt. Eine Einwilligung bedeutet allerdings ein Opt-in. Ein Opt-out reicht hierfür gerade nicht. Aber auch ohne Einwilligung könnte die Verwendung von Cookies unter der DS-GVO zulässig sein, gestützt auf Art. 6 Abs. 1 lit. b) DS-GVO zum Beispiel bei Cookies, die für den Vertragsschluss oder als vorvertragliche Maßnahme erforderlich sind, etwa wenn der Nutzer eine Ware in den Warenkorb verschiebt. Es wird zudem vertreten, Art. 6 Abs. 1 lit. f) DS-GVO als Rechtfertigung für die Cookie-Nutzung heranzuziehen, vorausgesetzt, es liegen berechnete wirtschaftliche, rechtliche oder ideelle Interessen des Verwenders vor, die nur bei Verwendung von Cookies erreicht werden können und denen gegenüber die Rechte der Betroffenen nicht entgegenstehen. Diese Interessen müssten dann ebenfalls in der Datenschutzerklärung benannt werden.

Es bleibt nach wie vor auf Klärung durch Leitfäden der Aufsichtsbehörden, Rechtsprechung und vor allem die ePrivacy-Verordnung zu hoffen.

V. Sonderfall E-Mail-Werbung

In der Datenschutzerklärung muss auch über die Verwendung der E-Mail-Adresse im Zusammenhang mit E-Mail-Werbung hingewiesen werden. An die Zulässigkeit der Versendung solcher E-Mails werden jedoch noch weitere rechtliche Voraussetzungen geknüpft:

Zur Vornahme von E-Mail-Werbung ist in der Regel eine protokollierte Einwilligung erforderlich, welche zu erkennen gibt, dass es dem Nutzer bei Erklärung dieser Einwilligung bekannt gewesen ist, welche konkreten Waren oder Dienstleistungen von welchem Unternehmer beworben werden sollen. Dies kann mithilfe eines separaten „Opt-In“ auf der Webseite selbst erfolgen, also der Möglichkeit, sich unabhängig von laufenden Vertragsbeziehungen für den Werbe-Newsletter anzumelden. Für den Nachweis der erfolgten Einwilligung, den der Webseitenbetreiber zu führen hat, ist jedoch lediglich das „Double Opt-In-Verfahren“ geeignet. Das bedeutet, dass dem Kunden nach dessen Eintragung für den Newsletter zunächst eine E-Mail geschickt wird, die einen Bestätigungslink beinhaltet, den der Kunde betätigen muss. Denn ansonsten könne laut Rechtsprechung nicht gewährleistet werden, dass die Einwilligung auch tatsächlich durch den E-Mail-Empfänger selbst und nicht einen unbekanntem Dritten erteilt wurde.



Zudem muss der Nutzer spätestens mit der Einwilligungserteilung auf die bestehende Widerrufsmöglichkeit hingewiesen werden. Der Newsletter selbst muss zudem ebenfalls darauf hinweisen und eine einfache Möglichkeit hierzu bieten, entweder per Link auf eine Abmeldeseite, oder eine E-Mail-Adresse speziell zur Abmeldung. Unzulässig ist es, die Einwilligung allein mittels E-Mail-Anfrage einzuholen, da dies bereits eine unzulässige Datennutzung ohne vorherige Einwilligung darstellt.

Eine Ausnahme des Einwilligungserfordernisses für E-Mail-Werbung-Werbung bestimmt das Gesetz für den Fall, dass der Unternehmer die E-Mail-Adresse im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden erhalten hat, er diese E-Mail-Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet, der Kunde der Verwendung nicht widersprochen hat und dieser bei Erhebung der E-Mail-Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann. Da im Falle des Verstoßes jedoch wettbewerbsrechtliche Abmahnungen und Unterlassungsklagen drohen, sollte in jedem Einzelfall ganz genau geprüft werden, ob und wann sich auf diese Ausnahme berufen werden kann.

Weitere Informationen hierzu finden Sie in unserem Merkblatt „[Telemarketing](#)“.

VI. Rechtliche Folgen

Mit der DS-GVO sind die drohenden Sanktionen im Fall von Datenschutzverstößen noch einmal empfindlich angezogen worden. So stehen nun den betroffenen Personen auch Schadensersatzansprüche gegen den Verantwortlichen zu. Gleichzeitig kann die Aufsichtsbehörde Geldbußen verhängen, deren Höhe je nach Verstoß und Einzelfall bis zu 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs betragen können. Je nach Verstoß drohen zudem Freiheitsstrafen (§ 42 BDSG n.F.), die Entziehung der Gewerbeerlaubnis, wettbewerbsrechtliche Abmahnungen oder auch Unterlassungsklagen der betroffenen Kunden. Mit der DS-GVO kommen nun auch ein Verbandsklagerecht und Schadensersatzansprüche der Betroffenen, sodass die Einhaltung der Regeln auch aus wirtschaftlicher Sicht an Bedeutung noch einmal stark zunimmt.

Zuständige Behörde für die Ahndung von Verstößen gegen das Telemediengesetz mittels Bußgeldern ist die Bezirksregierung Düsseldorf.

Das Thema Datenschutz im Internet und Datenschutzerklärung ist sehr komplex und die Risiken durch die Sanktionsmöglichkeiten der Aufsichtsbehörden und Dritter enorm. Eine einzelfallbezogene Beratung ist hier oft unerlässlich.



Industrie- und Handelskammer
zu Köln

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

Stand: April 2018

Mitgliedsunternehmen der IHK Köln und solche Personen, die in der Region Köln die Gründung eines Unternehmens planen, erhalten weitere Informationen bei Ihren Ansprechpartnerinnen:

Zum Thema Datenschutz:

Birgit Wirtz
Tel. 0221 1640-3300
Fax 0221 1640-3380
E-Mail: birgit.wirtz@koeln.ihk.de

Zum Thema Internetrecht:

Susanne Wollenweber
Tel. 0221 1640-3100
Fax: 0221 1640-3190
E-Mail: susanne.wollenweber@koeln.ihk.de

Industrie- und Handelskammer zu Köln
Unter Sachsenhausen 10–26
50667 Köln
www.ihk-koeln.de

Bitte bewerten Sie das von Ihnen genutzte IHK-Merkblatt - [hier geht's zum kurzen Online-Fragebogen](#).

Vielen Dank für Ihr Feedback!