

Datenschutz PRAXIS

RECHTSSICHER | VOLLSTÄNDIG | DAUERHAFT

Oktober 2022

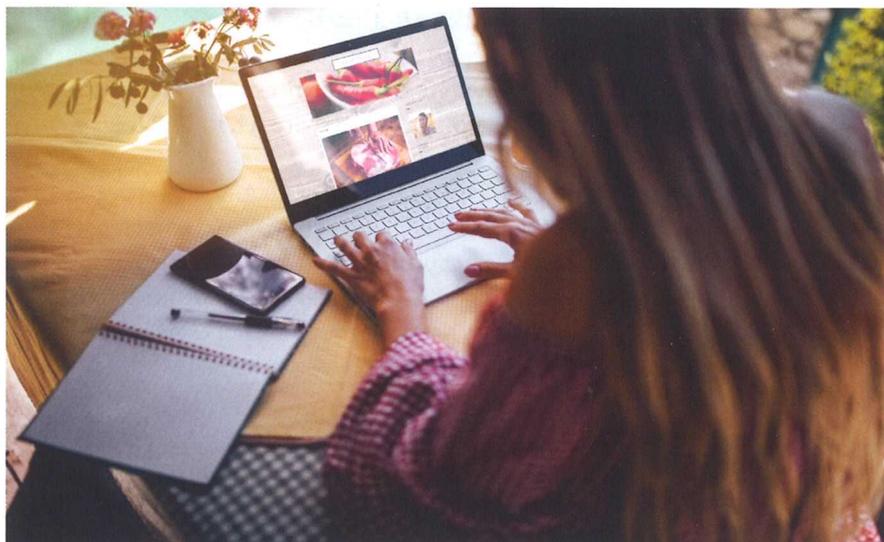


Bild: iStock.com/wundervisuals

Eine rechtskonforme Datenschutzerklärung ist ein Aushängeschild, gleich ob bei großen oder kleinen Unternehmen. Die nötige Zeit zu investieren, um sie korrekt zu gestalten, lohnt sich also. Zudem bietet eine rechtssichere Datenschutzerklärung keine Angriffsfläche für Abmahner.

Transparenz als oberstes Gebot

Datenschutzerklärung für Websites: Das muss drinstehen

Jedes Unternehmen mit einer Website muss transparent informieren, was es mit den dort verarbeiteten Daten tut. Wie lässt sich das in Zeiten von Abmahnungen wegen Google Fonts, von Analysetools, TTDSG und nötigen Belehrungen über Joint-Controller-Verhältnisse umsetzen?

Seit Dezember 2021 müssen Website-Betreiber die Vorgaben des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) beachten. Das TTDSG (dort § 25) gilt grundsätzlich vorrangig vor der Datenschutz-Grundverordnung (DSGVO), wenn es um das Auslesen und Speichern von Daten auf dem Endgerät von Nutzern geht – und das ganz unabhängig davon, ob es sich um

personenbezogene oder rein technische Daten handelt.

Sie als Datenschutzbeauftragte (DSB) und Verantwortliche müssen also die Zulässigkeit der Verarbeitung von Cookies, von Pixeln oder vergleichbaren Tools auf Websites seit Dezember auf zwei verschiedenen Ebenen beurteilen und auch in der Datenschutzerklärung darstellen:

- einerseits auf der Ebene des initialen Auslesens/Speicherns; dies ist grundsätzlich nach TTDSG zu beurteilen;
- andererseits auf der nachgelagerten Ebene der anschließenden Verarbeitung nach DSGVO (z.B. Analyse, Tracking).

Anpassungsbedarf nach TTDSG

Bestehende Datenschutzerklärungen sind daher unter Berücksichtigung des TTDSG anzupassen. Dabei ist die Rechtsgrundlage, die auf dem TTDSG basiert, bzw. der Hinweis auf die Einwilligung nach TTDSG nicht nur hinsichtlich der verwendeten Cookies und ähnlichen Tools zu ergänzen, sondern auch schon bei der Verarbeitung von technisch erforderlichen Daten – sofern das TTDSG Anwendung findet.

Welche Angaben die Datenschutzerklärung konkret enthalten muss, ergibt sich im Einzelnen aus Art. 13 und 14 DS- →

GVO. In der Praxis hat sich durchgesetzt, neben den Minimalangaben nach Art. 13 Abs. 1 DSGVO auch die weiteren Angaben nach Abs. 2 aufzunehmen.

Zudem hat sich aufgrund der Fülle der Informationen durchgesetzt, dass Texte jeweils unter einer Überschrift aufklappbar sind. Überlegen Sie, hier den Umgang mit Daten von Kunden und Geschäftspartnern außerhalb des Internets darzustellen. So lässt sich (jedenfalls ergänzend) in Allgemeinen Geschäftsbedingungen oder im Footer einer geschäftlichen E-Mail auf die Website verweisen. Wesentlich ist immer, dass die Informationen transparent und leicht verständlich sind.

Checkliste: Was sollte die Datenschutzerklärung enthalten?

1. Informationen über den oder die Verantwortlichen

Verantwortlicher ist üblicherweise das Unternehmen, das im Impressum der Webseite angegeben ist. Diese Kontaktadresse gehört auch in die Datenschutzerklärung. Während es früher üblich war, nur einen Verantwortlichen zu benennen, kommt es

im Einklang mit der Rechtsprechung des Europäischen Gerichtshofs (EuGH) insbesondere bei Social-Media-Seiten häufig zu einer gemeinsamen Verantwortlichkeit mit dem jeweiligen Anbieter der Plattform. Dann muss die Datenschutzerklärung diese Anbieter zusätzlich nennen und deren Kontaktdaten aufführen.

Es empfiehlt sich, gesonderte Social-Media-Datenschutzerklärungen zu erstellen und darauf zu verlinken, um intransparente Darstellungen zu vermeiden.

2. Kontaktdaten des/der Datenschutzbeauftragten

Der oder die Datenschutzbeauftragte ist namentlich zu benennen. Als Kontaktadresse bietet sich die geschäftliche Adresse des Verantwortlichen an; ggf. empfiehlt sich eine allgemein gehaltene E-Mail-Adresse, die speziell dem Datenschutz zugeordnet wird (datenschutzbeauftragte@...).

3. Zwecke der Verarbeitung

Die Datenschutzerklärung muss u.a. eine ausführliche Information über onlinetypische Nutzungen wie den Einsatz von Cookies, Social Plug-ins, Tracking- oder

Profiling-Tools, enthalten. Besteht eine gemeinsame Verantwortlichkeit, gehört auch hinein, wie der Joint Controller mit den Daten umgeht. Um die Transparenz zu wahren, empfiehlt es sich, zu unterscheiden, ob jemand

- die Website lediglich besucht,
- die dortigen Services aktiv nutzt oder
- eine Social-Media-Plattform besucht.

Ist Letzteres der Fall, gehört ein Verweis auf die Datenschutzinformationen des jeweiligen Plattform-Betreibers in die Erklärung. Zudem hat sich für Cookies eine eigene Erklärung durchgesetzt.

Zweck: Informatorische Nutzung

Beim reinen Besuch einer Website ist es üblicherweise nicht erforderlich, dass jemand Angaben zu seiner Person machen muss, also sich z.B. registriert oder seine Kontaktdaten angibt. Doch auch in diesen Fällen erhebt der Website-Betreiber personenbezogene Daten. Das ist der Fall, wenn er z.B. für die Verbesserung der Funktionalitäten der Website, deren Optimierung oder Analyse Daten sammelt. Hier ist eine sorgfältige Information über

alle eingesetzten Tools Pflicht. Dies kann z.B. umfassen:

■ Information über die technische Bereitstellung

Üblicherweise verarbeitet eine Website bestimmte, automatisch übermittelte Informationen, damit der Browser des Nutzers die Website und ggf. das Cookie-Banner anzeigen und nutzen kann. Dazu gehören z.B. IP-Adresse, Browsertyp/-version, Informationen zum JavaScript und zur Zugriffs-Uhrzeit. Diese Daten speichert das System in Serverlogfiles.

■ Information über Cookies

Wer Cookies einsetzt, sollte erläutern, was ein Cookie ist, wie es funktioniert und wozu er die Cookies nutzt. Außerdem ist wichtig, welche Informationen die Cookies speichern und übermitteln (z.B. Spracheinstellungen, Suchbegriffe, Dauer der Speicherung). Die Datenschutzerklärung erläutert idealerweise, wie der Nutzer Cookies ausschaltet. Hier ist ein Hinweis auf die entsprechenden Funktionalitäten oder auf die Hilfedatei des Browsers empfehlenswert, zusätzlich auf die Seite www.allaboutcookies.org. Unerlässlich ist zudem ein Hinweis auf die Konsequenzen: Schaltet ein Besucher Cookies aus, führt dies meist dazu, dass er nicht mehr alle Funktionen nutzen kann.

Setzt die Website nicht nur technisch notwendige Cookies ein, sondern auch Dienste, die nicht unbedingt für die Funktionalität erforderlich sind, ist im Einklang mit der Rechtsprechung des EuGH beim ersten Aufruf der Website eine Einwilligung in die Datenverarbeitung erforderlich. Dies erfolgt regelmäßig über ein Cookie-Banner, eine Cookie-Wall o.Ä.

■ Information über eingesetzte Analysetools etc.

Setzt der Website-Betreiber Analysetools ein wie Google Analytics, Facebook Pixel, Salesforce etc., kann er u.a. das Surfverhalten des Nutzers analysieren. Achten Sie darauf, ausführlich über die Funktionen der Analysetools, die Möglichkeiten z.B. der Anonymisierung der IP-Adresse

zu informieren bzw. darüber, dass entsprechende Einstellungen im Browser die Speicherung von Cookies verhindern können. Daneben ist – wie oben bereits ausgeführt – über das Cookie-Banner eine Einwilligung des Nutzers erforderlich. Die Zwecke sind möglichst konkret zu nennen (siehe Gailus, Ausgabe 05/22, S. 1–4, www.datenschutz-praxis.de/grundlagen/zweckbestimmung-wie-konkret-muss-sie-ausfallen/).

■ Information über Social-Media-Plug-ins

Sofern eine Website Plug-ins von Internetnetzwerken wie Facebook, Twitter oder Instagram nutzt, ist ein Hinweis auf deren Datenschutzerklärung unerlässlich, da sie regelmäßig eigenständig Daten erheben bzw. übermitteln. Social Plug-ins einzusetzen, ist rechtlich höchst kritisch. Denn sowohl die Rechtsprechung als auch die Datenschutzaufsichtsbehörden erachten die Weiterleitung von Daten an die Anbieter der Social-Plug-ins ohne ausdrückliche vorherige Einwilligung in der Regel als unzulässig. Egal, wie ausführlich oder gut die Belehrung ist: Ein Restrisiko verbleibt.

Zweck: Aktive Nutzung der Website

Daneben muss der Anbieter sorgfältig über den Umgang mit Daten informieren, die er bei der Nutzung der Online-Services verarbeitet. Dazu zählen z.B. Online-Shops, Online-Bewerbungen, die Teilnahme an Gewinnspielen oder Umfragen,



ACHTUNG!

Rein vorsorglich sei darauf hingewiesen, dass selbst mit Einwilligung diverse Tools – v.a. des US-amerikanischen Anbieters Google Inc. – inzwischen als kritisch einzustufen sind. Denn mangels Rechtsgrundlage findet eine unzulässige Übermittlung von Daten an Google statt. Insofern ist hier besondere Vorsicht geboten bzw. der Betreiber müsste idealerweise eine Einwilligung in die Übermittlung der Daten in die USA einholen – doch das ist technisch nur schwer möglich und rechtlich umstritten.

die Bestellung von Newslettern, aber auch Downloads von Materialien oder die Kontaktaufnahme mit dem Service-Center. Es ist inzwischen üblich, auch über Themen zu belehren wie den Umgang mit Daten

- aufgrund gesetzlicher Vorgaben (z.B. die Archivierung von geschäftlicher Korrespondenz oder Rechnungen),
- im Zusammenhang mit der Rechtsdurchsetzung (z.B. wenn das Unternehmen Forderungen einziehen will) oder
- bei einem Unternehmensverkauf.

4. Information über Links

Meist arbeiten Webauftritte mit Links, die auf Webseiten Dritter verweisen. Hier ist ein Hinweis auf den Haftungsausschluss sinnvoll und darauf, dass deren Datenschutzerklärungen für diese Inhalte gelten.

5. Information über Social Media

Daneben empfiehlt sich eine eigene Erklärung für Social Media, auf die die Datenschutzerklärung verlinkt. Hier ist v.a. die gemeinsame Verantwortlichkeit zwischen dem Anbieter der Plattform und dem Betreiber der Website hervorzuheben und welche Verarbeitungen wer vornimmt (z.B. Veröffentlichung von Rezensionen, Beantwortung von Nutzeranfragen oder Teilen von Inhalten). Ein Link auf die Datenschutzerklärung der Social-Media-Anbieter ist zwingend. Im Übrigen muss diese die nach Art. 13, 14 DSGVO üblichen Informationen enthalten.

6. Rechtsgrundlagen

Achten Sie darauf, für sämtliche Zwecke die jeweiligen Rechtsgrundlagen anzugeben. Hier sind einerseits die Rechtsgrundlagen aus der DSGVO relevant, andererseits die aus anderen Gesetzen wie dem TTDSG oder dem Jugendschutzgesetz.

Informatorische Nutzung der Website

So ist z.B. bei der technischen Bereitstellung der Website und der Cookie-Banner jetzt ein Hinweis auf § 25 Abs. 2 Nr. 2 TTDSG erforderlich. Der Hinweis sollte darüber belehren, dass die Verarbeitung der Daten unbedingt erforderlich ist, damit der Anbieter die ausdrücklich ge- →

wünschte Nutzung der Website (d.h. ohne oder mit Cookies) ermöglichen kann.

Verarbeitet der Verantwortliche Daten zur statistischen Analyse und zur Reichweitenerhöhung, muss er nun darüber informieren, dass die Verarbeitung einerseits aufgrund der Einwilligung nach § 25 Abs. 1 TTDSG hinsichtlich des initialen Speicherns und Auslesens von Daten und andererseits aufgrund der Einwilligung gemäß Art. 6 Abs. 1 Buchst. a DSGVO für die weitere Datenverarbeitung (z.B. Bereitstellung von Funktionalitäten, Analysen, Tracking, Optimierung etc.) erfolgt.

Idealerweise sagt die Datenschutzerklärung dem Nutzer, wie er seine Einwilligung widerrufen kann. Besucht der Nutzer die Seite, um sich über Produkte oder Veranstaltungen zu informieren, ist als Rechtsgrundlage Art. 6 Abs. 1 Buchst. b DSGVO anzugeben. Denn die Nutzung dient dann der Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen. Weiterhin bietet sich ein Hinweis auf Art. 6 Abs. 1 Buchst. f DSGVO an, wenn die Verarbeitung zur Wahrung der berechtigten Interessen erfolgt. Die berechtigten Interessen (z.B. Schutz vor Cyberangriffen) sind anzugeben.

Aktive Nutzung der Website

Hier ist im Einzelfall zu prüfen, auf welcher Rechtsgrundlage die Verarbeitung für die jeweiligen Zwecke basieren kann. Beispiele:

- Bei einem Onlineshop oder bei der Teilnahme an einem Gewinnspiel lässt sich auf Art. 6 Abs. 1 Buchst. b DSGVO (= erforderlich für die Erfüllung vertraglicher Zwecke) Bezug nehmen.
- Ergänzend kann sich bei einem Gewinnspiel auch eine Rechtfertigung aus Art. 6 Abs. 1 Buchst. c DSGVO in Verbindung mit § 661a Bürgerliches Gesetzbuch (BGB) ergeben: Der Anbieter eines Gewinnspiels unterliegt einer rechtlichen Verpflichtung, den Preis im Fall eines Gewinns auch zu leisten.
- Der Bezug des Newsletters wird sich aus Art. 6 Abs. 1 Buchst. a DSGVO – der Einwilligung – rechtfertigen lassen.



ONLINE-TIPP

Eine zusammenfassende Checkliste finden Sie unter www.datenschutz-praxis.de/betroffenenrechte/cl-datenschutzerklaerung.

7. Empfänger der Daten

Die Datenschutzerklärung muss darstellen, welche Kategorien von Empfängern (z.B. Agenturen, IT-Dienstleister, Banken, öffentliche Stellen, Rechtsanwälte) warum Daten erhalten (z.B. für Zwecke der Vertragsabwicklung, zur Erfüllung gesetzlicher Vorgaben zur Auskunft oder als Auftragsverarbeiter). Dies umfasst auch den Austausch von Daten innerhalb eines Konzerns.

8. Übermittlung in unsicheres Drittland

Ebenso informiert die Datenschutzerklärung über die Übermittlung der Daten an Anbieter wie die Google Inc. und die Rechtsgrundlagen bzw. die angemessenen Garantien, die der Verantwortliche umgesetzt hat, um den Transfer zu legitimieren (z.B. Standarddatenschutzklauseln, Einwilligung; siehe Art. 44 ff. DSGVO).

Da Transfers insbesondere in die USA kritisch sind, wird z.T. vertreten, dass Website-Anbieter ausdrücklich z.B. über Risiken aus dem Cloud-Act informieren müssen. Verfolgen Sie hierzu die Rechtsentwicklung, um die Erklärung bei Bedarf zeitnah anzupassen. Das gilt v.a., weil die Rechtsprechung betroffenen Personen bereits Schadenersatzansprüche aufgrund des unzulässigen Transfers von Daten in die USA zugesprochen hat und aktuell Unternehmen vor einer Abmahnwelle stehen.

9. Quelle der Daten

Erhebt der Verantwortliche die Daten nicht direkt bei den betroffenen Personen, sondern z.B. über Dritte wie Auskunftsteien oder eine Suchmaschine, muss er über die Herkunft der Daten informieren.

10. Speicherung von Daten

Die Speicherdauer der Daten, die sowohl nur bei einem Besuch als auch bei aktiver Nutzung der Website anfallen, ist jeweils

anzugeben. Geben Sie möglichst konkrete Zeitfenster an und – sofern möglich – auch einen Hinweis, auf welcher Rechtsgrundlage die Speicherdauer beruht.

11. Rechte der betroffenen Person

Art. 12 ff. DSGVO sehen diverse Rechte vor, die die betroffene Person gegenüber dem Verantwortlichen geltend machen kann. Informieren Sie ausführlich über diese Rechte und ihren Umfang. Der Hinweis auf die speziellen Widerspruchsrechte nach Art. 21 DSGVO – z.B. bei Direktwerbung oder berechtigten Interessen – sollte zusätzlich gesondert und hervorgehoben, etwa eingerahmt, erfolgen.

12. Beschwerderecht

Benennen Sie neben dem Beschwerderecht an sich die Kontakte für diese Beschwerde, d.h. die zuständige Datenschutzaufsichtsbehörde und sich als DSB (idealerweise mit Kontaktdaten).

13. Verpflichtung, Daten bereitzustellen

Die Datenschutzerklärung muss darüber informieren, ob eine betroffene Person für bestimmte Zwecke wie den Abschluss eines Vertrags Daten bereitstellen muss und welche Konsequenzen die Weigerung hat, etwa dass der Vertrag dann nicht zustande kommt. Daneben empfiehlt sich ein Hinweis, ob Daten z.B. in einem Formular auf der Website zwingend oder freiwillig anzugeben sind.

14. Automatisierte Entscheidungsfindung/Profiling

Weiterhin ist eine Belehrung erforderlich, ob eine automatisierte Entscheidungsfindung oder ein Profiling stattfindet. Setzt die Website Analysetools ein, lässt sich das jedenfalls nicht ausschließen. Die Datenschutzerklärung sollte dann informieren, warum das Profiling erfolgt.

15. Einwilligung/Widerrufsrechte

Es ist über die Möglichkeit zu informieren, eine Einwilligung zu widerrufen.



Silvia C. Bauer ist Rechtsanwältin mit Schwerpunkt Datenschutz und Compliance bei der Luther Rechtsanwalts-gesellschaft mbH in Köln.