INFORMATION

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

21. April 2023

Wie geht ein datenschutzkonformer Internetauftritt?

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit informiert kompakt zum Datenschutz auf Webseiten.

Einen Internetauftritt zu betreiben ist heute komfortabler denn je. Standardisierte Angebote ermöglichen es z.B., auch umfangreiche Web-Shops mit wenig Aufwand online zu stellen. Nicht immer wird dabei auch an den Datenschutz gedacht. Häufig ist den Betreiber:innen nicht klar, worauf sie achten müssen und wie datenschutzrechtliche Anforderungen umgesetzt werden können.

Als Datenschutzaufsichtsbehörde ist uns bewusst, dass diese Materie nicht leicht zu verstehen ist. Mit dieser Handreichung möchten wir deshalb über die wesentlichen Aspekte des Betriebs von Webseiten aufklären und den Weg zu mehr Datenschutz erleichtern. Eine individuelle Beratung kann dies nicht ersetzen. Wer tiefer in das Thema einsteigen möchte, findet am Ende Verweise zu weiteren Hilfestellungen.

In dieser Handreichung gehen wir auf folgende zentrale Themen ein:

1. Wann ist eine Einwilligung erforderlich?
2. Wie sollte ein Einwilligungsbanner gestaltet sein?
3. Wie können Drittinhalte eingebunden werden?
4. Worüber müssen die Nutzenden informiert werden?
5. Worauf ist beim technischen Betrieb zu achten?
6. Was droht, wenn Pflichten missachtet werden?

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str. 22, 20459 Hamburg
Tel.: 040/42854-4040 | Fax: 040/42854-4000
E-Mail: mailbox@datenschutz.hamburg.de | Internet: www.datenschutz-hamburg.de

Hamburg

1. Wann ist eine Einwilligung erforderlich?

Besucher:innen von Webseiten müssen unerwünschte und unnötige Zugriffe auf ihre Geräte (Computer, Tablets oder Mobiltelefone) nicht ungefragt hinnehmen. Dies ist die geltende Rechtslage. Solche Zugriffe erfolgen beim Einsatz von Cookies und anderen vergleichbaren Techniken (z.B. Web Storage oder Browser-Fingerprinting) auf Webseiten.

In den meisten Fällen müssen Anbieter:innen auf ihrer Website daher eine Einwilligung der Nutzenden einholen, bevor Cookies und Ähnliches eingesetzt werden. Das Speichern oder Abrufen von Informationen im Browser ist dabei regelmäßig nur nach einer solchen Einwilligung zulässig. So sieht es § 25 Absatz 1 TTDSG (Telekommunikation-Telemedien-Datenschutz-Gesetz) vor. Es verpflichtet die Webseitenanbieter damit, ihre Angebote entsprechend auszugestalten.

Eine Einwilligung ist ausnahmsweise nur dann nicht vorzusehen, wenn ein Cookie für die Erbringung des Dienstes „unbedingt erforderlich“ ist (§ 25 Abs. 2 Nr. 2 TDDSG). Dies ist allein im technischen Sinne zu verstehen und gilt z.B. für Cookies, die benötigt werden, sobald sich Nutzende bei ihrem Nutzerkonto anmelden. Der Einsatz von Nutzertracking zu Werbezwecken oder zur Verbesserung des Angebots mag wirtschaftlich sinnvoll und wünschenswert sein, erforderlich ist dies aber regelmäßig nicht, um Besucher:innen die Webinhalte anzeigen zu können.

Die Pflicht aus dem TDDSG, eine Einwilligung der Nutzenden einzuholen, gilt unabhängig davon, ob dabei personenbezogene Daten verarbeitet werden. Häufig jedoch ist der Einsatz von Cookies etc. mit einem Personenbezug verbunden, z.B. weil individuelle Kennungen vergeben oder persönliche Präferenzen gespeichert werden. In diesen Fällen kann es erforderlich sein, eine weitere Einwilligung nach der DSGVO einzuholen.

Gut zu wissen: Beide Einwilligungen (TTDSG und DSGVO) können gleichzeitig eingeholt werden, wenn entsprechende Informationen im Einwilligungsbanner enthalten sind (mehr dazu in Abschnitt 2).

Wichtig: Solange noch keine Einwilligung erteilt wurde, dürfen keine einwilligungsbedürftigen Zugriffe auf die Geräte erfolgen bzw. keine personenbezogenen Daten der Besucher:innen verarbeitet werden. Dies ist bei der technischen Ausgestaltung des Angebots unbedingt zu beachten. Erst wenn die Nutzenden eine Wahl getroffen haben, dürfen diejenigen Dienste eingebunden werden, für deren Einsatz die Zustimmung erteilt wurde.

2. Wie sollte ein Einwilligungsbanner gestaltet sein?

Einwilligungen auf Webseiten werden üblicherweise über sog. Banner eingeholt. Dies sind den Inhalten vorgeschaltete Dialogfenster, auf denen über die Verarbeitung von Cookies usw. informiert wird und den Nutzenden ein Wahlrecht eingeräumt wird.

Werden im Rahmen eines Webangebots ausnahmsweise keine einwilligungsbedürftigen Informationen verarbeitet, ist kein Einwilligungsbanner erforderlich.

In der Cookie-Banner-Gestaltung sind Betreiber:innen bezüglich des Designs, Farbe, Größe oder Kontrasten weitgehend frei. Auch ist es zulässig und häufig sinnvoll, Informationen auf mehrere Unterseiten zu verteilen. Die Freiheit der Gestaltung endet jedoch dort, wo Besucher:innen durch eine verwirrende Bannergestaltung zu einem bestimmten Verhalten – meistens zur Erteilung der Einwilligung mit „Alles akzeptieren“, „Ok“ etc. – bewegt werden sollen.

Erste Ebene eines Einwilligungs-Banners

Die Auswahlflächen auf der ersten Banner-Ebene sollten einheitlich gestaltet sein. Konkret bietet es sich an, eine pauschale Einwilligungsabfrage (z. B. „Alles akzeptieren“), eine gleich prominente Ablehnfunktion (z. B. „Alles ablehnen“) und ggf. eine Möglichkeit weiterer feingranularer Informationen vorzusehen:

Damit die Einwilligung informiert erfolgen kann,

1. müssen im Einwilligungsbanner die konkreten Zwecke der beabsichtigten Verarbeitung mitgeteilt werden, wie z. B. das Anlegen von Nutzungsprofilen oder die Datenverarbeitung außerhalb des Europäischen Wirtschaftsraums (Drittlandtransfer)
2. müssen die eingebundenen Drittanbieter benannt werden („unsere Partner“ ist nicht ausreichend)
3. muss ein Link auf die Datenschutzinformationen vorhanden sein, wenn die Datenschutz-Informationen wegen des eingesetzten Banners ansonsten nicht einsehbar wären
4. muss ein Hinweis vorhanden sein, dass die Einwilligung jederzeit widerrufen werden kann.

Welche Informationen können auf weiteren Ebenen des Banners erfolgen?

Detailliertere Informationen zur Verarbeitung personenbezogener Daten sollten sinnvollerweise auf weiteren Ebenen des Einwilligungsbanners mitgeteilt werden. Die sind Angaben wie z. B.:

- Name und Gültigkeitsdauer eingesetzter Cookies,
- Angaben zur verwendeten Technik (Cookie-Speicher, Web Storage),
- die mit der Datenverarbeitung verfolgten Zwecke,
- die Benennung der Unternehmen, die Informationen wie z. B. Cookies auf dem Endgerät platzieren,
- Angaben zur Rechtsgrundlage, die das Setzen dieser Informationen erlaubt.

Wenn die Angaben zu den eingesetzten Cookies und vergleichbaren Technologien nicht bereits über das Banner mitgeteilt wurden, muss eine Verlinkung zu den Datenschutzinformationen erfolgen. Der Link sollte bei längeren Datenschutzinformationen direkt in den Abschnitt führen, in dem diese Angaben auffindbar sind.

3. Wie können Drittinhalte eingebunden werden?

Drittinhalte werden von anderen Anbietern zur Verfügung gestellt und in die eigene Webseite eingebunden. Hierzu gehören beispielsweise:

- Karten-Dienste
- Videos
- Fonts (Schriften, die von externen Servern geladen werden)
- Tag Manger
- Social Media Einbindungen

Auch in Bezug auf diese Inhalte gilt das oben Gesagte: Grundsätzlich müssen auch hier Einwilligungen gemäß TTDSG und ggf. auch gemäß DSGVO eingeholt werden.

Soweit dies möglich ist, sollte die konkrete Einbindung technisch erst dann erfolgen, wenn die Nutzenden einen solchen Dienst explizit anfordern (z.B. ein Video betrachten möchten).

4. Worüber müssen die Nutzenden informiert werden?

Betreiber:innen von Webseiten müssen ihre Besucher:innen umfangreich informieren, wenn auf der Webseite personenbezogene Daten verarbeitet werden. Die in den Datenschutzhinweisen mitzuteilenden Angaben ergeben sich aus Artikel 12 und 13 DSGVO. Diese Informationen müssen von jeder Seite eines Webangebots aus leicht zugänglich sein. Das bedeutet auch, dass Datenschutzhinweise nicht vom Cookie-Banner verdeckt sein dürfen.

5. Worauf ist beim technischen Betrieb zu achten?

Neben den Inhalten sind bei einer Website auch die technischen Umstände des Betriebs relevant. Ein Web-Server muss sicher konfiguriert und administriert werden, und die Webseiten sind gegen bekannte Angriffe zu schützen.
Aus Sicht des Datenschutzes sind besonders die folgenden Punkte relevant:

Transportverschlüsselung

Werden personenbezogene Daten auf einer Website verarbeitet, ist eine Transportverschlüsselung per TLS (Transport Layer Security) vorzusehen. Die Verschlüsselung ist mit einem gültigen Zertifikat einer anerkannten vertrauenswürdigen Zertifizierungsstelle abzusichern. Abgelaufene oder selbst generierte Zertifikate erfüllen diesen Zweck nicht.
Dabei ist zu beachten, dass bereits Kontaktformulare, Suchfunktionen oder andere niederschwellige Interaktionsmöglichkeiten einen entsprechenden Verschlüsselungsbedarf auslösen.
Die Verpflichtung zur Verschlüsselung liegt beim Anbieter. Beim Versuch, das Angebot unverschlüsselt per „http“ zu nutzen, sollte daher umgehend auf das TLS-gesicherte Angebot weitergeleitet werden.

Server-Logging

Alle gängigen Web-Server erstellen standardmäßig Protokolle der einzelnen Seitenzugriffe, meistens im sog. Common oder Combined Log Format. Solche Log-Dateien stellen personenbezogene Daten dar, wenn sie die IP-Adresse oder wenn Request- oder Referrer-Informationen persönliche Daten enthalten (z.B. einen Nutzernamen oder einen personenbeziehbaren Suchbegriff).
Server-Logs dürfen daher nur im erforderlichen Umfang vorgehalten und nur für geeignete Zwecke wie die Gewährleistung eines sicheren Betriebs genutzt werden. Sobald sie für diese Zwecke nicht mehr benötigt werden, sind die Log-Einträge zu löschen oder vollständig zu anonymisieren. Eine feste Löschfrist ist gesetzlich nicht festgelegt. Für den Zweck des sicheren Betriebs der Webseite gelten sieben Tage als Richtwert. Eine regelmäßige Verknüpfung der Log-Einträge mit sonstigen Daten der Nutzenden ist nicht zulässig. Die Nutzenden müssen im Rahmen der Datenschutzinformationen auch über die Log-Policy informiert werden (siehe Punkt 4).

6. Was droht, wenn Pflichten missachtet werden?

Das TDDSG sieht in § 28 vor, dass mit einer Geldbuße bis zu dreihunderttausend Euro bestraft werden kann, wer die in Abschnitt 1 erwähnten gesetzlichen Pflichten missachtet. Die DSGVO sieht umsatzabhängig ggf. höhere Geldbußen vor. Zudem kann die zuständige Aufsichtsbehörde die

Herstellung eines rechtskonformen Betriebs verbindlich anordnen. Für Webseitenbetreiber:innen mit Sitz in Hamburg ist der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit die zuständige Aufsichtsbehörde.

Weiterführende Informationen

- Mehr zum Datenschutz bei Webseiten ist in der Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien zu finden.
- Fragen und Antworten rund um das Thema hat der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg zusammengestellt.
- Zu Abschnitt 5 sind umfangreiche Hinweise des BSI (Bundesamt für Sicherheit in der Informationstechnik) verfügbar.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str. 22, 20459 Hamburg
Tel.: 040/42854-4040
Fax: 040/42854-4000
E-Mail: mailbox@datenschutz.hamburg.de
Internet: www.datenschutz-hamburg.de