Vorstandsmaterialien

Datenschutz – FAQ 6

Deutschsprachige Gesellschaft für psychosoziale Onlineberatung

Datenschutz - FAQ

In den Datenschutz – FAQ werden die Fragen beantwortet, die am häufigsten im Zusammenhang mit vertraulicher Kommunikation mit Ratsuchenden unter Nutzung von Digitalmedien (eMail, Video-Tools etc.) gestellt werden.

Fragen zu den FAQs bitten wir an die Geschäftsstelle (geschaeftsstelle @dg-onlineberatung.de) zu richten.

Über Ihr Feedback zu den FAQs freuen wir uns.

Wichtiger Hinweis:

Die Inhalte wurden nach bestem Wissen recherchiert und zusammengestellt und ersetzen keine fachkundige Unterweisung. Für die hier veröffentlichten Inhalte übernimmt die DGOB keine Gewähr und keine Haftung.

Wegen der schnellen technischen Entwicklung und der darauf reagierenden Gerichtsentscheidungen bleibt der hier vorgelegte Überblick unvollständig und vorläufig. Die Texte orientieren sich an den von Praktiker*innen häufig gestellte Fragen (FAQs) und reflektieren rechtliche Auflagen aus Sicht der Anforderungen, die an Berufsgeheimnisträger*innen gestellt sind.

Ist von BDSG (Bundesdatenschutzgesetz) die Rede, ist immer die jeweils gültige Fassung ab 2018 gemeint.

Versionsstand: 1.0 (2020)

Frage 6: Welche Anforderungen sind an eine DS-GVO/BDSG-konforme Website zu stellen?

Wer mangels technischer Kenntnisse die Erstellung einer Website[1] an ein Unternehmen delegiert, unterstellt, das fertige Produkt entspreche den einschlägigen datenschutzrechtlichen Anforderungen (DS-GVO, BDSG, TMK und TKG). Oftmals stehen nur schmale Budgets für die Erstellung einer Website zur Verfügung, weshalb viele Dienstleister*innen auf so genannte Website Builder zurückgreifen[2]. Mit keinem dieser Verfahren ist ohne zusätzliche Anpassungen sichergestellt, dass das fertige Produkt den europäischen und nationalen Datenschutzvorschriften entspricht.

Zu unterscheiden sind Website und Webserver. An beiden Enden lauern datenschutzrelevante Gefahren, die für technische Laien nicht sofort erkennbar sind. Websites beinhalten eine Mischung aus Struktur- und Scriptcode. Während html vorgibt, wie der Browser die Inhalte anzeigt, werden komplexere Aufgaben (z.B. die Erfassung und Übermittlung von Daten in einem Kontaktformular) mit Scriptsprachen wie Javascript, php, VBScript realisiert. Weil die DS-GVO im Zusammenhang mit der Erfassung und Verarbeitung personenbezogener Daten „privacy by design“ fordert (Art. 5 DS-GVO in Verbindung mit Art. 25, § 71 BDSG), dürfen nur aktuelle (d.h. von den Herstellern gepflegte) Versionen zum Einsatz kommen, was für Techniklaien schwer kontrollierbar ist. Kommen icht länger unterstützte (abgekündigte) Versionen von Scriptsrpachen (php, JavaScript etc.) oder Datenbank-Maschinen (MySQL etc.) zum Einsatz, haben Angreifer leichtes Spiel: personenbezogene Daten können eingesehen und/oder entwendet werden. Eine Website mit veraltetem Code verstößt in eklatanter Weise gegen die Anforderung „privacy by design“ und muss als grob fahrlässig bewertet werden.

Um diesem Problem zu entgehen, muss der/die Berufsgeheimnisträger*in die beauftragte Firma schriftlich verpflichten, die Forderung nach „privacy by design“ zu erfüllen und sich die Umsetzung bei Abnahme des fertigen Produkts bescheinigen lassen, und zwar im Detail. Nur dann kann im Fall eines datenrechtlichen Verstoßes die Haftung (zumindest teilweise) an das Unternehmen abgetreten werden.

Webserver sind Programme, die auf einem öffentlich erreichbaren Computer installiert sind. Von außen erreichbare technische Systeme sind prinzipiell angreifbar. Weshalb Webserver immer auf dem technisch aktuellen Stand zu halten sind und sichergestellt werden muss, dass die Konfigurationshinweise von Expert*innen für Datensicherheit Beachtung finden. Es nutzt der aktuellste Webserver nichts, wenn eine Fehlkonfiguration einen sicheren Betrieb unterläuft. Eine Aufgabe, die für Laien kaum zu bewältigen ist. Zusätzlich sollte der Webserver durch eine Firewall geschützt werden, deren Konfiguration (Regeln) Spezialkenntnisse erfordert. Eine verschlüsselte

[1] Unter einer Website (site = Grundstück, Baustelle) versteht man die Ansammlung aller Konfigurations- und Skriptdateien eines Internetauftritts, deren öffentliche Inhalte unter Eingabe einer individuellen Internetadresse (z.B. dg-onlineberatung.de = Domain) aufgerufen werden können. Die Anzeige dieser Inhalte erfolgt in einem Browser.

[2] z.B. Wordpress, Wix, Jimdo etc.

Auslieferung der Inhalte des Webservers setzt die Installation eines kostenpflichtigen ssl-Zertifikats[3] voraus, das von den gängigen Browsern akzeptiert werden muss, wenn die Meldung „Diese Website ist unsicher“ vermieden werden soll - was dazu führen dürfte, dass Ratsuchende dieser Website nicht vertrauen.

Wer nicht über die erforderlichen IT-Kenntnisse für eine korrekte Implementierung eines Webservers und einer Firewall verfügt, ist gut beraten, einen so genannten „managed server“ zu mieten. Hier sorgt der Hoster[4] für einen datensicheren Basisbetrieb des Webservers (state of the art). Im Fall eines Verstoßes gegen datenschutzrechtliche Auflagen geht die Haftung (zumindest teilweise) auf den Hoster über, immer vorausgesetzt, mit dem Hoster wurde ein AV-Vertrag geschlossen (vergl. Frage 5). Verzichtet werden kann auf einen AV-Vertrag nur dann, wenn die Webseite keinerlei Interaktion[5] mit dem/der Besucher*in der Website vorsieht (statische Website).

Grundsätzlich gilt: werden auf einer Website personenbezogene Daten erhoben (z.B. Kontaktformular), muss der Datenaustausch zwischen Client und Server ssl-verschlüsselt[6] erfolgen (Art. 25 DS-GVO, § 64 BDSG). Mittlerweile sind verschlüsselte Websites Standard und ISO-zertifizierte Hoster werden unverschlüsselte Serverumgebungen nur noch ausnahmsweise anbieten.

Neben den Anforderungen von DS-GVO/BDSG verpflichten zwei weitere Gesetze Personen und Institutionen, die Tele-Dienste anbieten: das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG).

Welche Daten über die (natürliche oder juristische) Person der Anbieter*innen veröffentlicht werden müssen (Anbieterkennzeichnung / Impressum), regelt der § 5 des TMG.

Außerdem verpflichtet das TMG die Anbieter*innen, dass sie eindeutig kenntlich machen, ab wann Ratsuchende einen Vertrag mit dem/der Anbieter*in eingehen (Transparenzgebot). D.h. Ratsuchende müssen einem Vertragsschluss explizit zustimmen. Es wird aus der kurzen Aufzählung deutlich, dass das TMG und DS-GVO/BDSG in einem Ergänzungsverhältnis zueinander stehen.

Weiterhin regelt das TMG im § 14 den Umgang mit Bestandsdaten. Unter die Bestandsdaten fallen alle Daten, die a) der inhaltlichen Ausgestaltung des Vertragsverhältnisses dienen (z.B. vollständiger Name, Bankverbindung, Rechnungsadresse etc.) und b) für die Nutzung der eingesetzten Telemedien erforderlich sind (z.B. Anmeldeinformationen, Accountdaten etc.).

Im § 15 TMG wird der Umgang mit den Nutzungsdaten geregelt. Nutzungsdaten sind Daten, die auf technischem Wege zustande kommen, z.B. die in den Logfiles des Webservers gespeicherten Daten, die für einen bestimmten/bestimmbaren Zeitraum gespeichert werden müssen (vergl. § 76 BDSG). Wird beispielsweise das Online-Angebot auf der Grundlage der jeweiligen Nutzungsdauer (in

[3] z.B. ComSign, DigiTrust, GlobalSign
[4] z.B. 1&1, Hetzner, HostEurope etc.
[5] Rein statische Websites dürften im Zusammenhang mit Beratungsangeboten selten vorkommen, weil seitens der Ratsuchenden ein (datensicheres) Angebot zur Kontaktaufnahme erwartet wird.
[6] Eine funktionierende ssl-Verschlüsselung wird durch das vorgestellte „https://“ signalisiert.

Minuten) bepreist, fällt die Protokollierung der Verbindungsdauer unter die Nutzungsdaten. Nutzungsdaten dürfen ausschließlich zweckgebunden erhoben werden.

Zum Thema „Speicherung“ von personenbezogenen (Nutzungs-/ Bestands-)Daten gilt: nur so viel und so lange speichern, wie es für die beruflichen/vertraglichen Zwecke notwendig ist.

Die Datenschutzkonferenz empfiehlt, alle Verbindungsdaten (insbesondere die IP-Adresse, Session-Cookies) nach Ende der Sitzung auf dem Webserver automatisch zu löschen. Müssen die Daten zu vertraglichen Zwecken zwischengespeichert werden, gibt die Datenschutzkonferenz eine Speicherfrist von derzeit 7 Tagen als Richtlinie vor (https://www.datenschutzkonferenz-online.de/datenschutz.html).

Berufsgeheimnisträger*innen oder Institutionen müssen beachten: Wird gespeichert, können Dritte (Rechtsanwält*innen, Gerichte etc.) Auskunft über die gespeicherten Daten verlangen. Umgekehrt gilt: „Was nicht gespeichert ist, muss auch nicht beauskunftet werden!“

Das TKG ist in Bezug auf die §§ 88 und 89 relevant. § 88 regelt das Fernmeldegeheimnis, das auch als Brief- oder Postgeheimnis bekannt ist. Schon die Auskunft, ob jemand an einer Telekommunikation beteiligt war, unterliegt dem Fernmeldegeheimnis. Ruft jemand beispielsweise die Telefonseelsorge an, darf die Rufnummer des/der Anrufer*in nicht gespeichert werden (das Angebot ist kostenlos, ein wichtiger Grund zur temporären Speicherung von Nutzungsdaten entfällt). Ergänzend zur Verpflichtung des § 88 TKG regelt der § 89 TKG, dass dem Fernmeldegeheimnis unterliegende Informationen auch dann nicht veröffentlicht werden dürfen, wenn man zufällig in deren Besitz gelangt (z.B. als Folge technischer Übermittlungsfehler etc).

Wer das Abhörverbot missachtet, indem er fremde Daten ausspäht (z.B. Hacker), wird gemäß § 202a StGB mit Geldstrafen oder Freiheitsentzug bestraft. Gleiches gilt für das unbefugte Abfangen von Daten (§ 202b StGB). Wer rechtswidrig Daten löscht, unbrauchbar macht oder verändert, wird ebenfalls bestraft (§ 303a StGB). Für diese Fälle des Datendiebstahls und der Datenspionage haften die Berufsgeheimnisträger*innen in ihrer Rolle als Diensteanbieter*innen nicht.

Aus der Aufzählung der einschlägigen Regelungen wird deutlich, dass es für Berufsgeheimnisträger*innen viele gute Gründe gibt, im Zusammenhang mit der Erhebung und Speicherung personenbezogener Daten unbedingt die datenschutzrechtlichen Grundprinzipien zu beachten:

1) Datenvermeidung und Datensparsamkeit und

2) Zweckbindung und Rechtmäßigkeit.

Um einen aufgerufenen Inhalt (im Deutschen vielfach als „Webseite“[7] bezeichnet) ausliefern zu können, braucht der Webserver die IP-Adresse des Client. Eine IP-Adresse ist bei privater Nutzung von Netzservices eine auf Zeit[8] vergebene Kennung (z.B. 192.130.34.222), bestehend aus vier Trippeln mit 1 bis 3 Ziffern, die den Rechner, aber nicht die den Rechner bedienende Person identifiziert. Handelsübliche Router benutzen außerdem ein Verfahren namens NAT (net address translation), weshalb nur die öffentliche IP-Adresse des Routers mitgeteilt wird. Im Oktober 2016 hat der EuGH geurteilt, IP-Adressen sind als personenbezogene Daten einzustufen und daher entsprechend zu schützen. Müssen IP-Adressen längerfristig gespeichert werden, ist dies nur erlaubt, wenn die IP-Adresse verschlüsselt[9] gespeichert wird. Verboten ist die anlasslose unverschlüsselte Speicherung von IP-Adressen. Wer diese Adressen unverschlüsselt speichern will, muss gute Gründe vortragen, warum und wozu diese Angaben benötigt werden, beispielsweise zur Gefahrenabwehr im Zusammenhang mit den Vorschriften des § 138 StGB (Nichtanzeige geplanter Straftaten).

Ein weiterer Punkt ist der gesetzeskonforme Einsatz von Cookies[10]. Die Informationspflichten gegenüber den Website-Besucher*innen sind abhängig von der Art des zu setzenden Cookies:

a) Session-Cookies/essentielle Cookies: sie werden gesetzt, wenn eine Verbindung zu einer Datenbank aufgebaut werden muss (z.B. nach der Anmeldung mit seinen/ihren Zugangsdaten),
b) Konfigurations-Cookies, z.B. zur Speicherung der Auswahl der angezeigten Sprache, wenn die Website mehrsprachig ist,
c) First-party-Cookies dienen der Wiedererkennbarkeit des/der Besucher*in (genauer: des Computers),
d) Third-party-Cookies sind Cookies, die auf Angebote Dritter verweisen (z.B. die häufig sichtbaren Verweise auf Werbeangebote Dritter),
e) SuperCookies oder Evercookies: wie der letzte Name schon sagt, werden diese Cookies dauerhaft und vor allem versteckt gespeichert, dass sie von den Nutzenden nicht so leicht entdeckt und entfernt werden können. Datenrechtlich handelt es sich um rechtswidrige Cookies, weil sie alle Nutzungsaktivitäten speichern und an Dritte übermitteln. Sie sind eine echte Bedrohung der Privatsphäre.
Eine weitere Unterscheidung betrifft die Dauer der Speicherung von Cookies:

[7] „Webseite“ ist die umgangssprachliche Bezeichnung für eine Scriptdatei, die Inhalte zwischen einem öffnenden <hmtl>-Tag und einem schließenden </html>-Tag codiert und unter einem Namen in einem Ordner abgespeichert wird. Der Aufruf eines Script erfolgt über einen Link.
[8] Statische IP-Adressen werden in der Regel nur von Firmen oder großen Institutionen genutzt. Hier ist der Personenbezug eingeschränkt, weil die Rechner im Firmennetzwerk über private IP-Adressen angesprochen werden, die nicht im Internet geroutet werden und die in jedem LAN vorkommen können (NAT = net address translation).
[9] Eine verschlüsselte Speicherung liegt dann vor, wenn das letzte Tripel durch „xxx“ ersetzt wird, weil der konkrete Kundenbezug (Name und Anschrift der Kund*in, Nutzungsdauer und Dokumentation, welche Websites aufgerufen wurden etc.) über das letzte Tripel herstellt wird.
[10] Cookies (auch http-Cookies) sind kleine Textdateien, die zwischen Server und Clients ausgetauscht werden, um Webanwendungen nutzerfreundlicher zu gestalten. Cookies speichern zum Beispiel die Adresse einer aufgerufenen Website, die Suchanfragen oder die Zeit, wie lange jemand eine Website besucht usw. Cookies dienen vor allem dem Internet-Marketing und dienen der Wiedererkennung der Nutzenden (genauer: der Widererkennung des Computers). Hat jemand auf einer Website nach Laptops gesucht und danach für eine bestimmte Zeit beim Aufruf des Browsers (ungefragt) Werbung für Laptops erhalten, hat er/sie dies Cookies zu verdanken. Cookies sind jedoch keine Schadroutinen, auch wenn dies immer wieder behauptet wird.

a) Transiente Cookies[11] (z.B. Session-Cookies) werden nur für die Dauer der Session (Browsersitzung) gespeichert und nach Beenden der Session (Logout) aus Sicherheitsgründen gelöscht, damit nicht unbefugte Dritte das Session-Cookie kapern können und sich so Zugang zum Account des/der Nutzend*en verschaffen können.
b) Persistente Cookies besitzen eine lange Lebensdauer oder bleiben dauerhaft gespeichert. Das Setzen persistenter Cookies verstößt gegen die Auflagen der DS-GVO/BDSG, weil mit persistenten Cookies in der Regel die Privatsphäre ausgespäht wird.

Ob und welche Cookies gesetzt werden, muss der/die Website-Betreiber*in in der Datenschutzerklärung mitteilen und für zustimmungspflichtige Cookies eine solche Möglichkeit vorhalten. Technisch notwendige „essentielle" Cookies (z.B. Session-Cookies) dürfen auch ohne explizite Zustimmung der Website-Besucher*innen gesetzt werden. Es ist hilfreich, den Begriff „essentiell" sehr eng auszulegen. Alle anderen Cookies (z.B. Cookies zu Statistikzwecken) dürfen erst nach (!) expliziter Zustimmung (opt-in) der Website-Besucher*innen gesetzt werden. Was voraussetzt, dass für alle Cookies die Standardeinstellung auf „nein" gesetzt ist (default)[12].

Häufig ist auf Webservern so genannte Tracking-Software[13] installiert. Datenschutzrechtlich ist gegen statische Erhebungen nichts einzuwenden, soweit die dazu notwendigen Daten rechtskonform erhoben und ohne Personenbezug gespeichert werden. Viele der von USA-Firmen entwickelten Web-Tracker erheben Daten, die das Nutzungsverhalten der Website-Besucher*innen ausspähen und damit anderen Zwecken dienen. In den AGBs der Tracking-Software ist festgelegt, dass eine Nutzung an die Zustimmung der Übertragung der gesammelten Daten an Webserver außerhalb der EU gekoppelt ist (vergl Kopplungsverbot, Art. 7 Absatz 4 DS-GVO, § 28 Absatz 3b BDSG). Der Einsatz von Trackern wird seitens der deutschen Datenschützer kritisiert und hat in einem ersten Schritt dazu geführt, dass alle staatlichen und halbstaatlichen Einrichtungen verpflichtet wurden, auf die Installation solcher Tracker zu verzichten.

Um Ratsuchenden das Auffinden der Beratungsräumlichkeiten zu erleichtern, wird häufig auf Online-Kartendienste wie Google-Maps zurückgegriffen. Bei der Einbindung wird vielfach übersehen, dass die Aktionen der Website-Besucher*innen ab Aufruf der Website erfasst und ungefragt an Google USA übermittelt werden, ohne dass die Website-Besucher*innen davon Kenntnis haben und diesem Vorgehen widersprechen könnten. Zusätzlich setzt Google bei der Nutzung von Maps NID-Cookies[14]

[11] https://www.datenschutzbeauftragter-bayern.com/de/glossar/!/29/transiente-cookies/

[12] Der Vollständigkeit halber sei erwähnt, dass die aktuelle Auslegung der geltenden §§ 12 und 15 TMG das Setzen von Cookies mit voreingestellter Zustimmung für rechtmäßig ansieht. Die Datenschutzkonferenz sieht in dieser Auslegung einen Widerspruch zur geplanten ePrivacy-Richtlinie der EU und empfiehlt, auf ein opt-out Verfahren (= voreingestellte Zustimmung) vorsorglich zu verzichten (https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf und https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32002L0058&from=DE).

[13] Bekanntester Vertreter solcher Software dürfte Google-Analytics sein. Synonym ist der Begriff „Webalizer".

[14] In der Google-Datenschutzerklärung heißt es: „Google verwendet Cookies wie das NID- und das SID-Cookie, um Werbung in Google-Produkten wie der Google-Suche individuell anzupassen. Mithilfe solcher Cookies erfassen wir zum Beispiel Ihre neuesten Suchanfragen, Ihre bisherigen Interaktionen mit den Anzeigen

zu Werbezwecken. Aus Sicht der DGOB ist es berufsethisch bedenklich, wenn Berufsgeheimnisträger*innen auf ihrer Website PlugIns installieren, mit denen die Aktivitäten der Website-Besucher*innen ausgespäht und ungefragt an Dritte übermittelt werden. Erinnert sei an das Urteil des Bundesarbeitsgerichts (BAG, in Frage 2 zitiert), wonach bereits der Wunsch nach psychosozialer Beratung ein Privatgeheimnis darstellt, das von Berufsgeheimnisträger*innen gemäß § 203 StGB zu schützen ist. Wer auf die Idee kommt, statt des Karten-PlugIns lediglich einen Screenshot des Kartenausschnitts zu veröffentlichen, verstößt gegen die Nutzungsbedingungen und Urheberrechte von Google, was zur Abmahnung der Website-Betreiber*innen führen kann.

Die Einbindung von OpenStreetMap (OSM) hat zumindest den Vorteil, dass deren Server an Standorten innerhalb der EU (aber auch in Großbritannien, das demnächst kein EU-Mitglied mehr ist) betrieben werden. Allerdings werden auch bei OSM die IP-Adressen der Website-Besucher*innen gespeichert. Mit seinem Urteil hat das EuGH-Urteil klargestellt, dass die anlasslose Speicherung von IP-Adressen[15] rechtswidrig ist. Für die unverschlüsselte Speicherung von IP-Adressen müssen Website-Betreiber*innen triftige Gründe vorweisen.

Wie so oft gilt: weniger ist mehr, d.h. weniger Komfort für die Website-Besucher*innen trägt zum einem Mehr an Datenschutz bei.

Fazit:

Alleine der Umfang der Ausführungen zur Frage 6 macht deutlich: Die datenschutzrechtskonforme Gestaltung einer Website ist eine voraussetzungsvolle Angelegenheit, die man entweder in Zusammenarbeit mit spezialisiertem Fachpersonal durchführen sollte oder erst nach eingehender Recherche der aktuell gültigen datenschutzrechtlichen Vorgaben (DS-GVO und BDSG). Die hier aufgezählten Punkt erheben nicht den Anspruch auf Vollständigkeit, nicht zuletzt, weil jedes neue Gerichtsurteil auf nationaler und europäischer Ebene neue Verhältnisse schafft und neue Verpflichtungen definiert oder bestehende Verpflichtungen neu definiert.

---

eines Werbetreibenden oder den Suchergebnissen und Ihre Besuche auf der Website eines Werbetreibenden. Auf diese Weise können wir Ihnen individuell zugeschnittene Werbung auf Google anzeigen.“ (https://policies.google.com/technologies/types?hl=de).

[15] Das Vorgehen stellt einen Verstoß dar, auch wenn die unverschlüsselten IP-Adressen nicht bei dem/der Berufsgeheimnisträger*in selbst gespeichert werden, sondern bei Dritten. Durch die Einbindung solcher PlugIns wie Google-Maps machen sich die Berufsgeheimnisträger*innen zur Erfüllungsgehilf*innen für einen im Prinzip rechtswidrigen Vorgang.

Kontakt:
DGOB
Geschäftsstelle
Ernst Reuter Str. 8a
67373 Dudenhofen
Tel. 06232 / 312 86 33

Zitationshinweis:

DGOB: Datenchutz-FAQs Frage 6, 2020

Webabruf: https://