Deutschsprachige Gesellschaft
für psychosoziale Onlineberatung

Datenschutz - FAQ

Die Fragen 1 bis 6

In einem Dokument

Version 1 / April 2020

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 1: Es wird behauptet, handelsübliche eMail-Programme dürfen für die vertrauliche Kommunikation mit Ratsuchenden nicht genutzt werden. Stimmt das?

Handelsübliche, d.h. in die Betriebssysteme integrierte, eMail-Programme wie Outlook, Apple-Mail, Android-Messenger (Programme auf der Basis der Protokolle pop, smtp, imap) tauschen in der Standardkonfiguration eMails ohne Ende-zu-Ende-Verschlüsselung aus. Dadurch wird ein einfacher Austausch von eMails über Betriebssystemgrenzen hinweg (Windows, Apple macOS/iOS, Android etc.) möglich. Kommt es zur Übermittlung personenbezogener Daten, müssen ~~die~~ Kund*innen der Übermittlung vorab zustimmen (Anerkennung der AGBs und der Datenschutzrichtlinien des Anbieters).

Beratungsfachkräfte zählen gemäß § 203 StGB[1] zu den Berufsgeheimnisträger*innen. Für sie gelten besondere Auflagen im Umgang mit Privatgeheimnissen. Sie werden durch die Norm des § 203 StGB ***einseitig*** verpflichtet, ihnen anvertraute Privatgeheimnisse zu wahren (Schweigeverpflichtung). Berufsgeheimnisträger*innen ist auferlegt, durch geeignete organisatorische und technische Maßnahmen sicherzustellen, dass die Kommunikation zu jedem Zeitpunkt und über jeden genutzten Kommunikationsweg/-kanal vertraulich erfolgt und eine Offenbarung der anvertrauten Geheimnisse nicht unbefugt[2] erfolgt.

Berufsgeheimnisträger*innen und vertrauliche Kommunikation:

Eine Verschlüsselung von eMails setzt den Einsatz spezieller Zusatzprogramme oder PlugIns voraus[3]. Eine einwandfreie Funktion erfordert notwendigerweise, dass das gewählte technische Verfahren auf beiden (!) Seiten, d.h. beim Sender und Empfänger, korrekt implementiert ist. Ist dies auf einer Seite nicht der Fall, gibt es zwei Möglichkeiten: im besten Fall wird der Versand der eMail unterbunden, im schlimmsten Fall wird die eMail unverschlüsselt versendet, ohne dass der Sender darüber (explizit) informiert wird. Weil kein*e Berufsgeheimnisträger*in einseitig sicherstellen[4] kann, dass Ratsuchende a) zu ihrem Betriebssystem kompatible Verschlüsselungstechnik einsetzen und b) in der Lage sind, deren einwandfreie Funktion sicher zu stellen, ***verbietet*** sich wegen dieser Unwägbarkeiten der Versand sensibler Informationen via eMail. Beim Einsatz von eMail-Kommunikation nimmt der/die Berufsgeheimnisträger*in billigend oder (grob) fahrlässig in Kauf, dass anvertraute Geheimnisse offenbart werden (können), weil mit eMail übertragene Informationen prinzipiell abgefangen werden können. Wenn die Informationen dann noch unverschlüsselt

[1] https://www.gesetze-im-internet.de/stgb/__203.html
[2] Eine unbefugte Offenbarung liegt vor, wenn a) das fremde Geheimnis Dritten (Person, Institution) mitgeteilt wird, ohne dass eine Einwilligung vorliegt oder b) ein (technischer) Kommunikationsweg gewählt wurde, der die Vertraulichkeit der Kommunikation nicht durchgehend (!) gewährleistet.
[3] z.B. PGP / sMIME etc.
[4] „Sicherstellen“ bedeutet in diesem Zusammenhang, dass bereits vor der ersten (und spontanen) Kontaktaufnahme via eMail geprüft werden müsste, ob der eMail-Austausch verschlüsselt erfolgt.

vorliegen, nimmt der/die Berufsgeheimnisträger*in die Offenbarung in Kauf[5]. Selbst die zufällige[6] Offenbarung des anvertrauten Privatgeheimnisses stellt eine Straftat dar und kann mit einer Geld- oder Gefängnisstrafe geahndet werden.

Einige technische Anmerkungen zur eMail-Kommunikation:

Viele der einseitig beim Sender installierten PlugIns verschlüsseln lediglich den Anhang (Anlagen) der eMail. Enthält die eMail personenbezogene Daten, werden diese unverschlüsselt übertragen. Techniklösungen dieser Art sind für eine vertrauliche Kommunikation gänzlich ungeeignet.

Die häufig beworbene verschlüsselte Übertragung von eMails inklusive aller Anhänge vermittels TLS / SSL (so genannte Transportverschlüsselung) garantiert zunächst nur die verschlüsselte Übertragung zwischen Client (hier: Rechner der Berufsgeheimnisträger*in) und Server (Rechner des Service- oder Mailproviders[7]). Ob der sich anschließende Weitertransport der eMail auf dem Weg zum/zur Empfänger*in ausschließlich über TLS-verschlüsselte Netzknoten (Hubs/Relais) führt, ist dagegen nicht garantiert[8]. Selbst wenn es auf nur einer Teilstrecke zu einer unverschlüsselten Übertragung der eMail kommt, können unbefugte Dritte den Inhalt mitlesen, speichern und sogar manipulieren. Außerdem kann es sein, dass ab jetzt die eMail unverschlüsselt übertragen wird. TLS ist nicht gleichbedeutend mit Ende-zu-Ende-Verschlüsselung!

Ende-zu-Ende-Verschlüsselungen[9] erfordern den zeitlich vorgängigen Austausch eines öffentlichen Schlüssels (public key) zwischen den Clients und setzen die (kostenpflichtige) Installation eines Sicherheitszertifikats[10] voraus. Auch der Umweg über so genannte Schlüsselserver funktioniert nur für vorab beim Schlüsselserver registrierte Clients. Eine spontane, aber dennoch vertrauliche

[5] Es gilt, zwischen grob fahrlässiger, fahrlässiger und billigender Inkaufnahme zu unterscheiden. Grob fahrlässig wäre ein unverschlüsselter Austausch von Informationen im Zusammenhang mit einer vom Ratsuchenden begangenen Straftat, deren Bekanntwerden negative Folgen für die betroffene Person hat. Fahrlässig wäre ein unverschlüsselter Austausch, wenn nicht sichergestellt ist, dass der sensible Inhalt der eMail nur von der Adressat*in gelesen werden kann. Billigende Inkaufnahme der Offenbarung liegt vor, wenn die Berufsgeheimnisträger*in auf ihrer Website darauf hinweist, dass die Übermittlung sensibler Informationen via eMail unsicher ist, im Falle der Wahl dieses Kommunikationsweges die Ratsuchenden selbst für eine evtl. erfolgende Offenbarung verantwortlich sind. Eine (individuelle) Entpflichtung aus den Auflagen des § 203 StGB ist nicht möglich.

[6] Zufällig wäre eine Offenbarung auf Grund temporärer technischer Fehler (z.B. versehentlicher Versand der eMail ohne Verschlüsselung, weil die Fehlfunktion zu diesem Zeitpunkt unentdeckt blieb).

[7] Es sei erwähnt, dass Web-Dienstleister wie z.B. web.de ausdrücklich darauf hinweisen, dass die Nutzung dieses kostenlosen Dienstes ausschließlich für private Zwecke erlaubt ist.

[8] Dies wäre nur dann der Fall, wenn beide Seiten ein VPN nutzen, was aber im Zuge einer spontanen Kontaktaufnahme nicht funktioniert. Für die Nutzung eines VPN müssen die Verschlüsselungs- und Anmeldeparameter vor (!) Aufbau der VPN-Verbindung beiden Seiten bekannt sein.

[9] durch Einsatz spezieller Programme wie beispielsweise PGP, sMIME oder spezieller PlugIns

[10] Angriffe auf Zertifikatsstellen (certificate authority) sind dokumentiert. Zudem gilt es zu bedenken, dass nicht jeder SSL-Zertifikatstyp für jeden Einsatzzweck gleich gut geeignet ist.

Kontaktaufnahme der Ratsuchenden ist mit keinem der bisher aufgezählten Verfahren datensicher möglich.

Wie bei jeder Technik finden sich auch bei Verschlüsselungssoftware Schwachstellen (Einfallstore für Hacker und Schadsoftware durch fehlerhafte Softwareupdate, Fehlfunktionen der Software, Hardwarefehler). Informationen zu bekannt gewordenen Schwachstellen finden sich u.a. bei EFAIL (efail.de). Auf Portalen wie diesen finden sich auch Informationen, ob und wann der Fehler behoben (gepatcht) wurde.

Um den zentralen Anforderungen an die Informationssicherheit[11] zu genügen, sind ausschließlich solche Verfahren zu wählen, die 1) eine verschlüsselte Ende-zu-Ende-Kommunikation gestatten (Vertraulichkeit durch Verschlüsselung) und 2) sicherstellen, dass eine Manipulation der übermittelten Informationen erkannt werden kann (Vertraulichkeit durch Datenintegrität). Datenintegrität kann unter Einsatz qualifizierter elektronischer Signaturen sichergestellt werden. Diese Technik gestattet die verschlüsselte Übertragung und macht Veränderungen des Inhalts während des Transports und nachträglich beim Empfänger sichtbar. „Elektronische Signatur“ ist ein Rechtsbegriff aus der Signaturrichtlinie[12]. Im Gegensatz dazu nutzt die „digitale Signatur“ eine beim Versand erzeugte Prüfsumme (Hash-Wert), mit dem sich zwar ebenfalls Veränderungen der übermittelten Information feststellen lassen, allerdings bleibt unaufgeklärt, an welcher Stelle die Manipulationen der Originaldaten erfolgten. Die Empfänger*in kann also nur wissen, dass es sich nicht um die Originaldaten handelt.

Vor allem wenn in der Kommunikation mit den Ratsuchenden Informationen von rechtlicher Bedeutung ausgetauscht werden (sollen), ist der Nachweis der Datenintegrität von besonderer Bedeutung (z. B. bei Beratung zu Straftaten in Verbindung mit einem laufenden oder drohenden Gerichtsverfahren).

Erwähnt sei noch, dass die eMail *das* Einfallstor für die Verbreitung von Schadroutinen (Viren, Trojaner, Keylogger etc.) darstellt. Gefahr geht vor allem von eMails aus (bis dato) unbekannten Quellen aus. Während Desktop-Betriebssysteme durch den Einsatz von (aktueller) Anti-Viren-Software gut geschützt werden können, gilt das für die auf Mobilgeräten (Smartphones, Tablets) installierten Betriebssysteme[13] nur eingeschränkt.

Werden Schadroutinen über eMail eingeschleust, ergeben sich Anschlussgefahren für die lokale IT-Infrastruktur durch Beschädigung und Diebstahl von lokal gespeicherten Daten, durch das böswillige Sperren des Computers oder Beschädigungen am lokalen Netzwerk (verbunden mit der Forderung nach Lösegeldzahlung) und durch Schadroutinen, mit denen die Aktionen der Nutzer*innen

[11] geregelt in der ISO/IEC-27000-Reihe.
[12] Richtlinie 1999/93/EG v. 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L 13 v. 19.1.2000
[13] Wie bei den Desktop-Systemen gilt auch hier, dass einige Betriebssystem auf Grund ihrer Architektur verwundbarer sind als andere.

ausgespäht werden (Keylogger zum Ausspähen von Passworteingaben). Auf diese Weise gelingt Unbefugten der Zugriff auf die gesamte Computer-Infrastruktur, selbst wenn sichere[14] Passwörter zum Einsatz kommen. Besonders gefährdet sind Computersysteme, die mit vom Hersteller abgekündigten Betriebssystem-Versionen betrieben werden, was im Zusammenhang mit der Verarbeitung besonderer Kategorien personenbezogener Daten[15] (Art. 9 DS-GVO) ein grob fahrlässiges Verhalten darstellt.

Fazit:

Solange amtlich zertifizierte Verfahren, wie sie im De-Mail-Gesetz[16] (vom 28.4.2011) beschrieben sind, nicht allgemein verfügbar und – zusätzlich – allgemein akzeptiert in Nutzung sind, scheidet die eMail für die Kommunikation zwischen Ratsuchenden und Berufsgeheimnisträger*innen aus.

Der/die Berufsgeheimnisträger*in haftet, wenn sie Kommunikationswege nutzt, die für eine vertrauliche Kommunikation ungeeignet sind. Um es noch einmal zu betonen: Berufsgeheimnisträger*innen können sich aus den Auflagen des § 203 StGB nicht entpflichten, etwa indem sie die Ratsuchenden auf die Gefahren der eMail-Kommunikation hinweisen und (paradoxerweise) diesen Weg zur Kontaktaufnahme dennoch anbieten.

Ganz grundsätzlich gilt, dass die Kontrolle über verschlüsselte und daten-integre Kommunikation via eMail nur dann als gegeben unterstellt werden darf, wenn technisch aufwendige Verschlüsselungsverfahren zum Einsatz kommen. Eine spontane Kontaktaufnahme von Ratsuchenden mit der Beratungsstelle über die auf der Website veröffentlichte eMail-Adresse ist dadurch aber ausgeschlossen, weshalb die aufwendigen eMail-Verschlüsselungsverfahren nicht praxistauglich sind. Der Einsatzzweck der veröffentlichten eMail-Adresse dient ja in erster Linie dazu, dass Ratsuchende Kontakt mit dem/der Berater*in (Berufsgeheimnisträger*in) aufnehmen können.

Wollen Berufsgeheimnisträger*innen auch (oder gerade) in Zeiten einer ungeregelten elektronischen Kommunikation aller mit allen glaubhaft vermitteln, dass die den Ratsuchenden zugesicherte Vertraulichkeit auch außerhalb des f2f-Kontaktes durch geeignete organisatorische und technische Maßnahmen umgesetzt und kontinuierlich sichergestellt wird, scheidet die (vertrauliche) Kommunikation über den (technisch) unsicheren eMail-Kanal aus. Wie dieser Sachverhalt den Ratsuchenden gegenüber kommuniziert werden kann, ist Inhalt der Frage 2.

[14] Sichere Passwörter sind nicht-triviale, nicht-lexikalische Kombinationen von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen wie Semikolon, Raute, Unterstrich etc.
[15] Im Zusammenhang mit psychosozialer Beratung kommt es häufig zur Erhebung und Verarbeitung besonderer Kategorien.
[16] https://www.gesetze-im-internet.de/de-mail-g/BJNR066610011.html. Zudem gilt gemäß §13 Absatz 7 TMG der Haftungsübergang auf den Diensteanbieter für unerlaubte Zugriffe, Verletzungen des Schutzes personenbezogener Daten und Störungen nach Angriffen von außen.

Frage 2: Über die auf der Website veröffentlichte eMail-Adresse haben Ratsuchende Kontakt aufgenommen und um Bekanntgabe eines Beratungstermins gebeten bzw. ihr Anliegen geschildert. Darf ich auf diese Anfrage antworten?

Am 13.1.1987 entschied das Bundesarbeitsgericht (BAG) rechtskräftig, dass bereits die Bekanntgabe (Mitteilung) des Wunsches nach psychosozialer Beratung ein Privatgeheimnis darstellt[17]. Folglich sind Berufsgeheimnisträger*innen verpflichtet, auf den Vortrag des Wunsches in einer Weise zu reagieren, die das Privatgeheimnis wahrt.

Erfolgt die Kontaktaufnahme mit der Berufsgeheimnisträger*in telefonisch, ist die Kommunikation durch die Vorgaben des § 88 TKG (Fernmeldegeheimnis) sowie die nachfolgende Norm des § 89 TKG (Abhörverbot) geschützt. Gleiches gilt für die Kontaktaufnahme mit einem Mobilgerät durch eine (kostenpflichtige) SMS, denn bei der SMS handelt es sich ebenfalls um einen Telekommunikationsdienst, der durch die vorstehend genannten Normen geschützt ist. Allerdings ist hier höchste Sorgfalt auf Seiten der Berufsgeheimnisträger*innen geboten. Auf Mobiltelefonen kommen proprietäre (vom Hersteller vorinstallierte) Messaging-Systeme zum Einsatz[18]. Die damit versendeten Nachrichten sind keine SMS im Sinne des TKG (Telekommunikationsgesetz). Bei manchen Mobilsystemen werden „echte“ SMS von proprietären Nachrichtendiensten durch eine andere Farbe[19] unterschieden.

Nehmen Ratsuchende via unverschlüsselter eMail Kontakt auf, verbunden mit dem Wunsch nach einem Beratungstermin oder einem Ratschlag, stellt die Beantwortung der Fragen unter Nutzung des gleichen (unverschlüsselten) Kommunikationsweges einen Verstoß gegen die Auflagen des § 203 StGB dar. Eine Kommunikation via eMail ist nur dann zulässig, wenn die Berufsgeheimnisträger*innen durch Einsatz geeigneter Technik (siehe Frage 1) sicherstellen kann, dass ab der Antwort der Austausch vertraulich[20] erfolgt. Der Wechsel von unverschlüsselter zu verschlüsselter Kommunikation erzwingt jedoch eine Änderung des technischen Verfahrens, worüber die Gegenseite – zunächst über den unverschlüsselten Kanal – informiert werden muss, was zu einer paradoxen Situation führt: der unverschlüsselten Antwort des/der Berufsgeheimnisträger*in kann entnommen werden, dass der Kontaktaufnahme ein Beratungswunsch zugrunde liegt, auf den gemäß BAG nur mit vertraulicher Kommunikation reagiert werden darf. Wie kann dieses Paradox aufgelöst werden?

[17] „Schon die Tatsache, dass jemand die Beratung des Klägers in seiner Eigenschaft als Berufspsychologe in Anspruch nimmt, ist ein Geheimnis im Sinne von 203 StGB und nicht erst das Problem, das Anlass für die Inanspruchnahme des Berufspsychologen ist.“ (AZR 267/85, Seite 8, Absatz 35).
[18] z.B. iMessage, WhatsApp etc.
[19] So werden SMS bei iOS-Systemen grün eingefärbt, das proprietäre Nachrichtenformat iMessage wird blau dargestellt.
[20] Wie in Frage 1 verdeutlicht, erfordert das Gebot der Vertraulichkeit nicht nur die Verschlüsselung der gesendeten Nachrichten, es muss darüber hinaus sichergestellt sein, dass nur die betroffene Person (exklusiven) Zugang zu den Nachrichten hat.

Formal korrekt ist eine Antwort der Berufsgeheimnisträger*innen via unverschlüsselter eMail, in der sie die Ratsuchenden in allgemeiner Weise über ihre Verpflichtung zur Wahrung des Privatgeheimnisses (Schweigeverpflichtung) informieren und – sofern vorhanden – auf einen sicheren Kommunikationsweg hinweisen, beispielsweise die Kommunikation über eine ssl-gesicherte Website oder eine datensichere Online-Beratungsplattform – ohne auf die in der eMail gestellten Fragen einzugehen. Ein Antworttext könnte wie folgt aussehen: „Sie haben mir über meine eMail-Adresse eine Nachricht zukommen lassen. Ich möchte Sie hiermit informieren, dass ich in meiner Funktion als Berufsgeheimnisträger*in zur Wahrung des Privatgeheimnisses verpflichtet bin (§ 203 StGB, Verschwiegenheitspflicht) und deshalb auf diesem Weg keine Fragen im Zusammenhang mit einer gewünschten oder laufenden Beratung beantworten darf. Dies geschieht auch zu Ihrem Schutz, weil eine vertrauliche Kommunikation unter Einsatz von eMail nicht sichergestellt werden kann. Ich darf Sie daher auf die folgende Möglichkeit aufmerksam machen: … (mit einem Link zu dem geschützten Angebot). Über diesen Weg können Sie mit mir vertraulich kommunizieren, weil hier Ihre und meine Nachrichten verschlüsselt übertragen werden. Ich würde mich freuen, wenn Sie von dieser Möglichkeit Gebrauch machen, die nur einen Mausklick entfernt liegt. Bitte schützen Sie Ihre Privatsphäre.“

Nachteilig an diesem Verfahren ist, dass einige Ratsuchende sich nach einer solchen Antwort nach Möglichkeiten umsehen werden, die aus ihrer Sicht einen „einfacheren“ Zugang zu den gewünschten Informationen/Hilfestellungen bieten. Und weil es diese Angebote gibt, die in Unkenntnis der hier vorgetragenen Sachlage psychosoziale Beratung via eMail anbieten, werden sie fündig.

Obwohl das hier vorgeschlagene Verfahren (scheinbar) in Widerspruch zur Forderung steht, Beratung müsse niedrigschwellig erreichbar sein, verdeutlicht seriöse psychosoziale Beratung nicht nur aus strafrechtlichen, sondern auch aus berufsethischen Gründen, dass die Vertraulichkeit der Beratung ihr Markenzeichen ist und daher absolute Priorität hat. Bereits im Jahr 1977 stellt das Bundesverfassungsgericht in einem Urteil fest: „*Die grundsätzliche Wahrung des Geheimhaltungsinteresses der Klienten ist Vorbedingung des Vertrauens, das sie um ihrer selbst willen dem Berater entgegenbringen müssen, und damit zugleich Grundlage für die funktionsgerechte Tätigkeit der Beratungsstelle, deren Beistand die Klienten brauchen*“[21] Dem ist nichts hinzuzufügen!

Die Feststellung gilt nicht nur für Beratungsstellen, sondern für alle im § 203 StGB genannten Berufsgeheimnisträger*innen und allen, die durch die Zusammenarbeit mit Berufsgeheimnisträger*innen zu beruflich tätigen Gehilf*innen werden.

[21] BVerfG 44/353 (https://www.servat.unibe.ch/dfr/bv044353.html)

Frage 3: Wenn die Kommunikation via eMail ausscheidet, welche technischen Wege stehen alternativ für die vertrauliche Kommunikation mit den Ratsuchenden zur Verfügung?

Betreiben Berufsgeheimnisträger*innen eine verschlüsselte Website (https), stehen günstige technische Voraussetzungen für Verfahren zur Verfügung, die eine vertrauliche Kommunikation mit Ratsuchenden ermöglichen.

Eine Website, die ein Kontaktformular vorhält, muss die dort erfassten (personenbezogenen) Daten gemäß Art. 32 DS-GVO[22] verschlüsselt übermitteln. Will der/die Berufsgeheimnisträger*in die Daten einsehen, kann das auf zweierlei Art erfolgen:

a) er/sie meldet sich am ssl-verschlüsselten Webserver an und sieht die Daten dort ein
oder

b) er/sie richtet eine verschlüsselte eMail-Verbindung zwischen Server und Computer ein[23], welche die Formulardaten verschlüsselt auf ihren Rechner überträgt.

Bei Zuwiderhandlung gegen die Auflagen der DS-GVO drohen beachtliche Bußgelder, wenn die/der Geschädigte nachweisen kann, dass ein ideeller oder materieller Schaden entstanden ist (Art. 82 DS-GVO).

Die technischen Voraussetzungen für die Einrichtung und den Betrieb eines verschlüsselten Webservers sind keineswegs trivial und sollte IT-Spezialist*innen[24] überlassen werden. Es bieten sich die nachfolgenden Möglichkeiten an:

a) man beauftragt eine IT-Firma mit der Einrichtung der für die Online-Beratung benötigten Tools[25], die idealer Weise nach ISO/IEC 27001 zertifiziert ist
oder
b) man greift auf zertifizierte Branchensoftware[26] zurück, die in der Regel auf einfache Weise in die bestehende Website „eingehängt“ werden kann.

[22] in Verbindung mit dem Art 5 DS-GVO, vergl. https://dsgvo-gesetz.de/

[23] Dieser Weg setzt voraus, dass die auf dem Server eingesetzte Software eine Aufbereitung des Inhalts des Kontaktformulars als eMail zulässt und dass die Verbindung zwischen Server und Client-Computer ssl-verschlüsselt ist. Auch hier ist ein SSL-Zertifikat (Port 993 bei imap, Port 995 bei pop) erforderlich und das lokale Mailprogramm darf eine ungesicherte Authentifizierung nicht erlauben. Für technisch nicht versierte Berufsgeheimnisträger*innen ist der Weg über das Web-Interface des Servers zu empfehlen.

[24] Wer selbst einen DS-GVO-konformen Web-Server einrichtet, haftet voll umfänglich für datenschutzrechtliche Verstöße, etwa wenn als Folge technisch unzureichender Maßnahmen personenbezogene Daten ungeschützt übertragen werden und/oder es zu einer Offenbarung dieser Daten kommt.

[25] (z.B. Möglichkeiten zur textgestützte Einzelberatung, Einzelchat oder Video-Konferenz)

[26] In Frage kommende Anbieter werden unter Eingabe der Suchworte „Software Onlineberatung“ oder „Onlineberatungssoftware“ gefunden. Als Folge der raschen technischen Entwicklung kommen immer wieder neue Anbieter dazu, während andere wegfallen. Auswahl der Software wie die vertragliche Absicherung der

Die Anbieter zertifizierter Branchensoftware übernehmen vielfach auch die Installation der Software auf einem ssl-verschlüsselten Webserver[27]. Mit dem Einsatz eines ssl-verschlüsselten Web-Servers gelingt die Zwangsverschlüsselung der gesamten Kommunikation zwischen Web-Server und Client ganz ohne Zutun der Besucher*innen der Website.

Mittlerweile haben (fach-)verbandliche Zusammenschlüsse dazu geführt, trägerübergreifende sichere eMailsysteme aufzusetzen[28]. Bislang vorliegende Erfahrungen zeigen, dass Ratsuchende sich von den „Umständen“ (Registrierungszwang, Abholen der Antworten jeweils nur nach Anmeldung am Server usw.) nicht abhalten lassen, mit der Beratungsstelle in Kontakt zu treten. Gegen das gängige Vorurteil, dass Ratsuchende es bevorzugten, via eMail Kontakt mit dem/der Berufsgeheimnisträger*in oder der Beratungsstelle aufzunehmen, könnte auf Grundlage der Erfahrungen mit eMail-Hosting argumentiert werden: Wird Ratsuchenden sofort ***und*** ausschließlich (!) eine abgesicherte Möglichkeit der Kontaktaufnahme angeboten, wird diese ganz selbstverständlich genutzt.

Stehen eMail-Hostingsysteme als mandantenfähige Versionen zur Verfügung, werden sie auch für Einzelpersonen (Selbstständige) interessant.

Abschließend bleibt anzumerken, dass einmal getroffene technische Verfahrensentscheidungen nicht für die Ewigkeit sind. Die zu einem Zeitpunkt X installierten Verschlüsselungstechniken sind kontinuierlich auf Aktualität zu überprüfen (privacy by default, Art. 5 DS-GVO in Verbindung mit Art. 25 DS-GVO), ebenso wie die eingesetzten Skriptversionen (z.B. php) und Webserver-Versionen (z.B. Apache-Webserver).

Beauftragung als berufsmäßig tätiger Gehilfe (AV-Vertrag) liegen im Verantwortungsbereich der Berufsgeheimnisträger*innen, die für Versäumnisse haften.

[27] SSL-Zertifikat werden von einer Zertifizierungsstelle (trust center) ausgestellt und sind kostenpflichtig. Nur Zertifikate bekannter Trust Centers werden von den handelsüblichen Browsern erkannt. Exotische oder selbst erstellte Zertifikate bewirken die Anzeige des Hinweises: „Diese Website ist nicht sicher“, obwohl der Datenaustausch zwischen Client und Server verschlüsselt erfolgt.

[28] eMail-Hosting, http://lag-bw.net/wp-content/uploads/2020/01/sicherEmail_Kommunikation.pdf.

Frage 4: Warum können Video-Chats mit Ratsuchenden nicht mit Programmen wie Skype, Zoom durchgeführt werden, obwohl die Hersteller eine Ende-zu-Ende-Verschlüsselung zusichern?

Die DS-GVO gestattet die Verarbeitung (Erfassung, Speicherung, Verarbeitung) personenbezogener Daten bei einem Cloud-Dienstleister ohne besondere Nachweise über die Einhaltung der Vorgaben der DS-GVO, wenn der Diensteanbieter seinen Sitz in der EU hat und dadurch ebenfalls den Auflagen der DS-GVO unterworfen ist. Auch wenn diese Firmen darauf hinweisen, dass sie die Anforderungen des (amerikanischen) privacy shield (http://privacyshield.gov/list) erfüllen, ist der Einbezug von Nicht-EU-Firmen als „berufsmäßig tätiger Gehilfe“ nur dann DS-GVO/BDSG-konform, wenn der/die Berufsgeheimnisträger*in gegenüber der zuständigen Datenschutzbehörde den schriftlichen Nachweis erbringen kann, dass sich die Firma zur Einhaltung der europäischen und insbesondere deutschen Datenschutznormen (BDSG 2018) verpflichtet und eine Zertifizierung gemäß ISO/IEC 27001 nachweisen kann. Eine solche Vereinbarung dürfte nur im Ausnahmefall möglich sein und bleibt mit rechtlich bedeutsamen Restunsicherheiten verbunden. Firmen, die in ihren AGBs die Zustimmung zur Sammlung bestimmter personenbezogener Daten verlangen (selbst wenn dies „nur“ in Form so genannter Metadaten erfolgt[29]), scheiden für die vertrauliche Kommunikation zwischen Ratsuchenden und Berufsgeheimnisträger*innen ohnehin aus. Um es in einem Satz zu sagen: Für Beratungszwecke scheiden alle Firmen aus, deren Firmensitz außerhalb der EU liegt, die sich nicht per AV-Vertrag als berufsmäßig tätiger Gehilfe verpflichten lassen.

Berufsgeheimnisträger*innen sind durch die Vorschriften des § 203 StGB einseitig zur Wahrung des Privatgeheimnisses verpflichtet und es vor unbefugter, versehentlicher oder ungewollter Offenbarung zu schützen. Das verlangt adäquate organisatorische und technische Verfahren/Prozeduren. Mit Blick auf technische Verfahren gilt, dass die Verarbeitung personenbezogener Daten durch Dritte nur in Verbindung mit einem Auftrag zur Datenverarbeitung (kurz: AV-Vertrag, Art. 28 DS-GVO, § 62 BDSG, § 203 Absatz 4 Satz 1 StGB) erfolgen darf. Seit der Änderung des § 203 StGB am 30. Oktober 2017[30] stellt der Einbezug berufsmäßig tätiger Gehilfen zur ordnungsgemäßen Ausübung der Diensttätigkeit keine Offenbarung dar (bzw. stellt eine Offenbarung dar, die straffrei bleibt[31]). Der rechtskonforme Einbezug berufsmäßig tätiger Gehilfen ist jedoch an Voraussetzungen geknüpft, eine davon ist der vertragliche Einschluss des Dritten durch Abschluss eines AV-Vertrages, in dem der/die Auftraggeber*in (= Berufsgeheimnisträger*in) dem Auftragnehmer (z.B. Cloud-Dinestleister) vorschreibt, wie die personenbezogenen Daten „im Auftrag“ verarbeitet werden (dürfen). Im Fall einer Prüfung der Berufsgeheimnisträger*in, der Beratungseinrichtung oder des Trägers durch eine*n Beauftragte*n der zuständigen Landesdatenschutzbehörde, muss die vertragliche Einbindung zwingend nachgewiesen werden.

[29] Typisch für solche Geschäftsmodelle ist, dass die Zustimmung bereits voreingestellt ist (so genanntes ‚opt out’), d.h. die Zustimmung muss aktiv abgewählt werden. Ein solches Vorgehen widerspricht der aktuellen ePrivacy-Richtlinie (Stand Dezember 2019).

[30] Bundesgesetzblatt 2017 Teil I Nr. 71: Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen

[31] Deutscher Bundestag, Drucksache 18/11936, Seite 19.

Firmen, die Programme wie Skype, WhatsApp etc. zur kostenfreien Nutzung anbieten, schließen keine (individuellen) AV-Verträge, weil – wie bereits erwähnt – die AGBs die Sammlung von Metadaten vorsehen, die durch Protokollierung und Auswertung der individuellen[32] Aktivitäten der Nutzer*innen entstehen. Außerdem schließen diese Firmen eine Haftung im Fall eines Datenverstoßes aus und verweigern somit eine zentrale Verpflichtung eines datenschutzkonformen AV-Vertrages. Die alleinige Tatsache einer Ende-zu-Ende-verschlüsselten Übermittlung der Inhalte reicht als Nachweis einer vertraulich geführten Kommunikation im Sinne der Auflagen des § 203 StGB nicht aus. Firmen, die im Rahmen ihres Geschäftsmodells Metadaten sammeln, scheiden nicht nur aus datenschutzrechtlichen, sondern auch aus berufsethischen Gründen aus. Aus Sicht der COREPER (ständige Vertretung der EU-Mitgliedsstaaten) ist das Vorgehen dieser Firmen rechtlich bedenklich, weil u.a. die voreingestellte Zustimmung (opt-out) zu einer datenschutzrechtlich problematischen Verarbeitung personenbezogener oder personenbeziehbarer Daten führt und dieses Vorgehen gegen die noch zu verabschiedende e-privacy Richtlinie[33] der EU verstößt.

Allgemein gilt: der Einsatz technischer Maßnahmen ist rechtlich und berufsethisch nur gerechtfertigt, wenn diese der gesetzlich geforderten, zumutbaren Datensicherheit entspricht (vergl. Art. 25 DS-GVO in Verbindung mit den §§ 64 und 35 BDSG). Für die Kommunikation mit Ratsuchenden dürfen nur solche Dienstleister herangezogen werden, die

a) eine Zertifizierung (bevorzugt der ISO/IEC-27000er Reihe) nachweisen können,

b) ihren Firmensitz innerhalb der EU haben,

c) die Technik (Server-Standort) ebenfalls innerhalb der EU betreiben und

d) mit den Einzelkunden DS-GVO/BDSG-konforme AV-Verträge abschließen (zum Inhalt solcher AV-Verträge siehe Frage 5).

Eine Zuwiderhandlung stellt einen eklatanten Verstoß gegen die Vorschriften der DS-GVO und des BDSG dar, der mit Geldstrafen geahndet wird und - je nach Schwere des Verstoßes - eine Veröffentlichung auf der Website des zuständigen Landesdatenschützers nach sich ziehen kann. Berufsgeheimnisträger*innen, die gegen die Vorgaben des § 203 StGB verstoßen, machen sich strafbar. Es genügt die verdachtsweise Anzeige einer beratenen Person, durch die (vermutete) Offenbarung ihres Privatgeheimnisses einen ideellen oder materiellen Schaden erlitten zu haben. Ganz gleich, wie das Gericht am Ende urteilt: das Vertrauen in die Vertraulichkeit der Beratungskommunikation wird in der Öffentlichkeit beschädigt, nicht nur in Bezug auf den/die

[32] Das Argument, dass Metadaten einzelnen Nutzer*innen nicht mehr zugeordnet werden können, stimmt insofern, dass zwar die Realidentität der Nutzer*in nicht unbedingt bekannt ist, aber die Kennung des von ihm/ihr genutzten Rechners (MAC-Adresse, IP-Adresse, Fingerprint, Geotargeting etc.). Benutzen Berufsgeheimnisträger*innen Programme, bei denen in Verbindung mit der Nutzung Metadaten gesammelt werden, riskieren sie die Vertraulichkeit der Kommunikation und nehmen die Offenbarung von Privatgeheimnissen billigend in Kauf.

[33] Die derzeitige Richtlinie hat den Status eines Entwurfs, der allerdings zeigt, welche Auflagen die Diensteanbieter künftig erfüllen müssen.

Berufsgeheimnisträger*in, der/die gegen die Vorschriften verstoßen hat, sondern auch in Bezug auf die gesamte Profession. Das gilt es zu bedenken.

Frage 5: Welche Anforderungen sind an einen AV-Vertrag zu stellen, der die Auflagen des § 203 StGB erfüllt?

Personen und Institutionen, die personenbezogene Daten erfassen und zur Durchführung der eigenen Tätigkeit einen (oder mehrere) Auftragsverarbeiter einbeziehen, müssen Art und Umfang dieses Einbezugs in so genannten TOMs (technisch-organisatorische Maßnahmen) dokumentieren. In den TOMs wird im Detail festgelegt, wie der/die Auftragverarbeiter*in die von der Auftraggeber*in erhobenen personenbezogenen Daten verarbeiten darf (Art. 30 Absatz 2 DS-GVO in Verbindung mit Art. 28 DS-GVO und Erwägungsgrund 78, §§ 62 und 64 BDSG). Weshalb die im Vertrag zur Datenverarbeitung im Auftrag (nachfolgend AV-Vertrag genannt) dokumentierten Anforderungen hinreichend genau formuliert sein müssen, damit ersichtlich ist, was dem/der Auftragverarbeiter*in erlaubt und was verboten ist. Die Prüfung, ob der/die Auftragverarbeiter*in die Gewähr für eine technisch wie organisatorisch einwandfreie Verarbeitung der personenbezogenen Daten bietet, obliegt der Sorgfaltspflicht der Auftraggeber*in (Art. 28 Absatz 1 DS-GVO). Er/Sie haftet für die Wahl des/der Auftragverarbeiters und damit auch für den Fall, dass der/die einbezogene berufsmäßig tätige Gehilf*in (§ 203 StGB Absatz 3) nicht über die erforderliche (technisch-organisatorischen) Qualifikationen verfügt.

Obwohl sich die hier zu klärenden Fragen mit dem Einzug Dritter als berufsmäßig tätige*r Gehilf*in beschäftigen, sei der Vollständigkeit darauf hingewiesen, dass für jede Person oder Institution, die personenbezogene Daten verarbeitet, die Vorgaben des Art. 30 Absatz 1 DS-GVO gelten. Sie haben ein Verzeichnis der Verarbeitungstätigkeiten zu führen, aus dem sich die Pflichten ableiten, die an den/die berufsmäßig tätigen Gehilf*inen ausgelagert werden können. In Umkehrung heißt dies: es können keine Tätigkeiten ausgelagert werden, die im Verzeichnis der Auftraggeber*innen nicht gelistet sind. Erinnert sei auch an den datenschutzrechtlichen Grundsatz, dass personenbezogene Daten nur erhoben werden dürfen, wenn die Erhebung rechtmäßig ist und zweckgebunden erfolgt. Weshalb im Verarbeitungsverzeichnis aufgeführt sein sollte, auf welcher (Rechts-)Grundlage die Datenerhebung erfolgt und zu welchem Zweck und durch welche organisatorisch-technische Maßnahmen die weisungsgebundene Verarbeitung der erhobenen Daten sichergestellt wird.

Viele Auftragverarbeiter bieten ihren Kund*inen die Möglichkeit, einen Standard-AV-Vertrag elektronisch zu schließen. Der/die Auftragverarbeiter*in signiert den Ausdruck des AV-Dokuments, der/die Auftraggeber*in unterzeichnet das ausgedruckte Dokument und nimmt es zu ihren Akten. Ist der/die Auftragverarbeiter*in auf die Verarbeitung personenbezogener Daten spezialisiert, wie sie üblicherweise im Umfeld medizinischer, sozialpädagogischer oder psychologischer Dienstleistungen entstehen, dürfte der standardisierte AV-Vertrag den geltenden Anforderungen (zumindest im Prinzip) entsprechen. Werden die nachfolgend aufgezählten Punkte durch den Standardvertrag nicht oder nur unzureichend abgedeckt, ist ein zusätzlicher (individueller) AV-Vertrag mit dem/der Auftragverarbeiter*in abzuschließen. Es empfiehlt sich die schriftliche Fixierung und die postalische Zustellung des Zusatzvertrages, damit bei einer Prüfung das vom/von der Auftragverarbeiter*in händig unterzeichnete Dokument vorgelegt werden kann.

In Art.28 DS-GVO (Erwägungsgrund 81) sind die verpflichtenden (Mindest-)Inhalte von AV-Verträgen gelistet:

- Gegenstand, Dauer der Verarbeitung,
- Art und Zweck der Verarbeitung der erhobenen Daten
- Kategorien der personenbezogenen Daten (vor allem, wenn besondere Kategorien erhoben werden, vergl. Art 9 DS-GVO), Kreis der betroffenen Personen,
- Auflistung aller Daten, die erhoben werden, zugeordnet zu den Zwecken, derentwegen sie erhoben werden (z.B. vollständiger Namen, vollständige Adresse, Angaben zum Anlass der Beratung etc.),
- Pflichten und Rechte der Berufsgeheimnisträger*innen (als Verantwortliche),
- Schriftlich fixierte Weisung, wie der/die Auftragverarbeiter*in die Daten zu verarbeiten hat (Umfang der Auftragsverarbeitung, Pflichten de/ders Auftragverarbeiter*in),
- Schriftlicher Nachweis, dass der/die Auftragsnehmer*in alle mit der Verarbeitung betrauten (befugten) Personen zur Vertraulichkeit verpflichtet hat und Nachweis darüber, dass die Verpflichtung den gesetzlichen Anforderungen an die Verschwiegenheitspflicht entspricht,
- Nachweis über die Art und Weise der Umsetzung der Sicherheit der Datenverarbeitung durch den/die Auftragnehmer*in,
- sofern der/die Auftragnehmer*in weitere Auftragnehmer*innen im Untervertragsverhältnis einbezieht: Nachweis, dass die mit dem/der Hauptauftragsverarbeiter*in festgelegten Bedingungen auch bei den Untervertragsverarbeiter*innen[34] Anwendung finden,
- Verpflichtung des/der Auftragverarbeiter*in, Verletzungen des Schutzes personenbezogener Daten unverzüglich anzuzeigen, sowohl gegenüber der betroffenen Person (Ratsuchende*r) wie gegenüber dem/der Auftraggeber*in,
- In diesem Zusammenhang: evtl. Benachrichtigung der zuständigen Aufsichtsbehörde (Landesdatenschützer*in) durch den/die Auftraggeber*in, wenn mit der Verletzung der Schutzrechte hohe Risiken für die Betroffenen und/oder die Auftraggeber*innen einhergehen[35],
- Durchführung einer Datenschutz-Folgeabschätzung durch den/die Auftragverarbeiter*in,
- Festlegung, wie die Löschung bzw. Rückgabe der beim/bei der Auftragverarbeiter*in gespeicherten Daten nach Beendigung des AV-Vertrages erfolgt,
- Vereinbarung der Möglichkeit, die Einhaltung der geforderten Verarbeitungsprinzipien vor Ort (in den Räumen) des/der Auftragverarbeiter*in zu prüfen ggfs. durch eine*n kundige*n Vertreter*in des/der Auftraggeber*in prüfen und bescheinigen zu lassen.

AV-Verträge enthalten den Inhalt der Weisungen detailliert und erhalten dadurch einen gewissen Umfang[36]. Bestandteil des AV-Vertrages (Anlage) sind auch die vom/von der Auftragverarbeiter*in ausgewiesenen TOMs.

[34] Die DGOB empfiehlt, auf Untervertragsverhältnisse zu verzichten, weil sich daraus eine Reihe rechtlicher Unwägbarkeiten ergeben.
[35] Zum Beispiel bei Beratungen im Zusammenhang mit laufenden oder anstehenden Strafverfahren (Drogendelikte, Kindeswohlgefährdung etc.)
[36] Beispiele für Musterverträge finden sich hier: https://www.lda.bayern.de/media/muster_adv.pdf, https://datenschutz.hessen.de/infothek/hinweise-und-muster-ds-gvo, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/01/muster_adv.pdf

Kommt es zu einem Verstoß gegen die auferlegten Pflichten durch nachweisliches Verschulden des/der Auftragverarbeiter*in, haftet diese*r für den evtl. entstandenen (und gerichtlich festgestellten) Schaden, sofern der AV-Vertrag eindeutige Regelung zum kritisierten Verstoß enthält.
Außerdem müssen Regelungen zu folgenden Fragen getroffen werden:

- Liegen die vom/von der Auftraggeber*in erhobenen Daten bei dem/der Auftragverarbeiter*in verschlüsselt vor, so dass sie von Dritten (ohne besondere Erlaubnis[37] der Auftraggeber*in) nicht eingesehen werden können?
- Liegt eine wirksame Einwilligung der Betroffenen zur Datenspeicherung vor und sind die Betroffenen in eindeutiger Weise über den Umfang, den Rechtsgrund und den Zweck der Erhebung und Speicherung informiert?
- Ist die Weitergabe der Daten für die Vertragserfüllung erforderlich (z.B. bei Abrechnung der erbrachten Leistung mit einem Sozialversicherungsträger) und haben die Ratsuchenden dieser Weitergabe zugestimmt bzw. (falls eine Zustimmung rechtlich nicht erforderlich ist) werden die Ratsuchenden über jede Weitergabe für jeden Einzelfall informiert?

Können die für Tätigkeit notwendigen Daten ohne konkreten Personenbezug erhoben werden (anonymisiert/pseudonymisiert), sind die DS-GVO-Vorgaben nicht mehr einschlägig.

Abschließend noch einige Stichworte für eine Gliederung der technisch-organisatorischen Maßnahmen:

- Können die notwendigen Daten von Beginn an anonymisiert/pseudonymisiert erhoben werden (vor allem dann, wenn besondere Kategorien i.S. des Artikels 9 DS-GVO erhoben werden)?
- Durch welche technischen Vorkehrungen gelingt die verschlüsselte Speicherung personenbezogener Daten beim/bei der Auftragverarbeiter*in?
- Wer hat bei dem/der Berufsgeheimnisträger*in und bei dem/der Auftragverarbeiter*in Zugang zu den Daten (namentliche Nennung der Zugangsberechtigten ist hilfreich) und wie ist der Zugang geregelt (diese Frage spielt vor allem dann eine Rolle, wenn die Beratung in Privaträumen stattfindet, zu denen auch andere Personen Zugang haben)? Kann der Zugang protokolliert werden und wenn ja, in welcher nachprüfbaren und manipulationsgeschützten Form? Wie ist der Dienstrechner gesichert, um Unbefugten den Zugang zu verwehren? Werden privater und beruflicher Gebrauch durch die Nutzung unterschiedlicher Hardware unterstützt?
- Wie ist der Zugang zum Cloud-System geregelt (ausreichend sicheres Passwort, getrennte Zugänge für weitere berechtigte Benutzer*innen)?
- Wie sind die Schreib- und Leserechte geregelt, wenn mehr als eine Person Zugang zu den in der Cloud gespeicherten Daten hat (Rechteverwaltung) und wer hat das Recht, diese Rechte zu administrieren?
- Wie werden Datenzugriffe und Datenänderungen fälschungssicher protokolliert?
- Wenn Cloud-Dienstleister als berufsmäßig tätige Gehilf*inen einbezogen werden: wie wird die Verfügbarkeit des Systems sichergestellt (z.B. bei Stromausfall, technische Wartungsarbeiten etc.)?
- Wie wird das Cloud-System gegen technische Fehler und Angriffe von außen geschützt (Vulnerabilität/Stabilität)?

[37] Ein Erlaubnisgrund wäre zum Beispiel technischer Support für einen bestimmten (!) Fall und nur für die Dauer der Lösung des technischen Problems. Die Erteilung einer pauschalen Erlaubnis ist rechtswidrig.

- Ist die komplette Wiederherstellung der gespeicherten Daten im Falle technischer Fehler, Angriffe von außen oder Zerstörung sichergestellt, durch welche Maßnahmen?
- Wie erfolgt die regelmäßige Überprüfung, Bewertung und Evaluierung des geforderten Sicherheitsniveaus und der Wirksamkeit der eingesetzten technischen Verfahren?
- Wie erfolgt die Dokumentation der technisch-organisatorischen Maßnahmen (elektronisch, papiergestützt)?

Fazit:

Der Abschluss eines AV-Vertrages ist in jeder Beziehung voraussetzungsreich:

1) Jede*r Berufsgeheimnisträger*in, der/die personenbezogene Daten automatisiert erfasst und verarbeitet, muss ein Verarbeitungsverzeichnis führen, aus dem hervorgeht, welche Daten auf welcher (Rechts-)Grundlage erhoben und verarbeitet werden und durch welche organisatorischen und technischen Maßnahmen sicher gestellt wird, dass die Zweckbindung gewahrt wird.

2) Das Verarbeitungsverzeichnis ist die Grundlage und Voraussetzung der Entscheidung, welche Tätigkeiten an den/die berufsmäßig tätigen Gehilf*inen („Dritten“) ausgelagert werden sollen und ausgelagert werden dürfen.

Mit der Verpflichtung zur umfangreichen und detaillierten Dokumentation konkretisieren sich die hohen Voraussetzungen, die an den Einbezug berufsmäßig tätiger Gehilf*inen gestellt sind (§ 203 Absatz 3 StGB).

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

Wer mangels technischer Kenntnisse die Erstellung einer Website[38] 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[39]. 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

[38] 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.

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

Auslieferung der Inhalte des Webservers setzt die Installation eines kostenpflichtigen ssl-Zertifikats[40] 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[41] 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[42] 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[43] 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

[40] z.B. ComSign, DigiTrust, GlobalSign
[41] z.B. 1&1, Hetzner, HostEurope etc.
[42] Rein statische Websites dürften im Zusammenhang mit Beratungsangeboten selten vorkommen, weil seitens der Ratsuchenden ein (datensicheres) Angebot zur Kontaktaufnahme erwartet wird.
[43] 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“[44] bezeichnet) ausliefern zu können, braucht der Webserver die IP-Adresse des Client. Eine IP-Adresse ist bei privater Nutzung von Netzservices eine auf Zeit[45] 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[46] 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[47]. 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:

[44] „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.
[45] 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).
[46] 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.
[47] 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[48] (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)[49].

Häufig ist auf Webservern so genannte Tracking-Software[50] 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[51]

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

[49] 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).

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

[51] 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[52] 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).

[52] 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 2020

Webabruf: https://