Vorstandsmaterialien

Datenschutz – FAQ 1

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 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.

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

Zitationshinweis:

DGOB: Datenchutz-FAQs Frage 1, 2020

Webabruf: https://