Vorstandsmaterialien

Datenschutz – FAQ 4

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: 2.0 (Mai 2021)

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[1]), 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[2] stellt der Einbezug berufsmäßig tätiger Gehilfen zur ordnungsgemäßen Ausübung der Diensttätigkeit keine Offenbarung dar (bzw. stellt eine Offenbarung dar, die straffrei bleibt[3]). 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.

[1] 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).

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

[3] 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[4] 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[5] 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

[4] 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.

[5] 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.

Im Februar 2021 hat der Berliner Beauftragte für Datenschutz und Informationssicherheit Hinweise zu Anbietern von Videokonferenzdiensten veröffentlicht, die unter dem nachfolgenden Link eingesehen werden können:

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf#page=4

Die gelisteten Programme / Programmanbieter wurden gemäß der folgenden Kriterien getestet:

1. Vertragsgestaltung: ist der angebotenen Standardvertrag oder der zu schließende AV-Vertrag DSGVO-konform?
2. Dienstleister: verarbeitet der Dienstleister die während einer Konferenz entstehenden Daten selbst (gemäß Auftrag) oder werden Untervertragsverarbeiter einbezogen, die entweder nicht genannt oder nicht genehmigt sind?
3. Export: werden die während der Konferenz entstehenden Daten (insbesondere IP-Adressen) in Drittländer exportiert? Werden die Kunden über den Export informiert?
4. EU-Cluster: isst die Verarbeitung der während der Konferenz entstehenden (personenbezogenen) Daten auf Server beschränkt, deren physikalischer Standort sich ausschließlich innerhalb der EU befindet?

Die DGOB empfiehlt für den Einsatz von Konferenzsoftware, die eine Ende-zu-Ende-Verschlüsselung zulässt.

Konferenzprogramme us-amerikanischer Hersteller wie Zoom, MS Teams, Cisco-Webex etc. kommen während der Pandemie in Schulen und in Behörden zum Einsatz, wodurch deren Nutzbarkeit für Beratungszwecke abgeleitet wird. Für den Austausch dienstlicher Angelegenheiten (z.B. Dienstbesprechungen) mag die jeweilige Verantwortliche zu dem Schluss kommen, dass der Einsatz dieser Programme gerechtfertigt ist, obwohl die Hersteller z.B. IP-Adressen an Länder außerhalb der EU exportieren (z.B. in die USA). Voraussetzungen für die Nutzung ist, dass die Teilnehmenden sich explizit einverstanden erklären, dass die während der Konferenz entstehenden Daten, speziell die IP-Adressen in ein Drittland außerhalb der EU exportiert und dort verarbeitet werden. Die mit diesen Herstellern geschlossenen Verträge sehen nicht vor, dass die Daten innerhalb der Karenzzeit auf Verlagen gelöscht werden können, womit der Einsatz dieser Programme gegen ein zentrales Recht der Betroffenen verstößt (Art. 17 DSGVO). Ebenfalls bleibt intransparent, zu welchen Zwecken die gesammelten Daten verarbeitet werden. Insofern ist es begrüßenswert, wenn immer mehr Landesdatenschutzbehörden den Einsatz dieser Programme monieren.

Mit den vorstehend genannten Programmen (siehe Bewertung der Berliner Landesdatenschutzbehörde) können folglich weder Beratungen noch Intervisionen/Supervisionen rechtskonform durchgeführt werden, vor allem dann nicht, wenn es während der Intervision/Supervision zur Nennung von Daten kommen kann, die eine Re-Identifikation der Realidentität von Ratsuchenden ermöglichen. Der Hinweis, die genannten Programme würden auch

von öffentlichen Stellen und Behörden eingesetzt, dürfte im Falle einer gerichtlichen Auseinandersetzung nicht vor einer Verurteilung schützen, weil das Schutzniveau der im Rahmen einer Beratung anfallenden persönlichen Daten und Privatgeheimnisse (vergl. § 203 StGB in Verbindung mit Art. 9 DSGVO) mit den Maßnahmen zur (technischen) Datensicherheit korrespondieren muss.

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

Zitationshinweis:

DGOB: Datenchutz-FAQs Frage 4, 2020

Webabruf: https://