Vorstandsmaterialien

Datenschutz – FAQ 5

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 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 die Auftragverarbeiterin die von der Auftraggeberin 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 der Auftragverarbeiterin erlaubt und was verboten ist. Die Prüfung, ob die Auftragverarbeiterin die Gewähr für eine technisch wie organisatorisch einwandfreie Verarbeitung der personenbezogenen Daten bietet, obliegt der Sorgfaltspflicht der Auftraggeberin (Art. 28 Absatz 1 DS-GVO). Er/Sie haftet für die Wahl des Auftragverarbeiters und damit auch für den Fall, dass die einbezogene berufsmäßig tätige Gehilfin (§ 203 StGB Absatz 3) doch nicht über die erforderliche (technisch-organisatorischen) Qualifikationen verfügt.

Obwohl sich die hier zu klärenden Fragen mit dem Einzug Dritter als berufsmäßig tätige Gehilfin 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 die berufsmäßig tätige Gehilfin ausgelagert werden können. In Umkehrung heißt dies: es können keine Tätigkeiten ausgelagert werden, die im Verzeichnis der Auftraggeberin 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 Kundinnen die Möglichkeit, einen Standard-AV-Vertrag elektronisch zu schließen. Die Auftragverarbeiterin signiert den Ausdruck des AV-Dokuments, die Auftraggeberin unterzeichnet das ausgedruckte Dokument und nimmt es zu ihren Akten. Ist die Auftragverarbeiterin auf die Verarbeitung personenbezogener Daten spezialisiert, die im Zusammenhang mit medizinischen, sozialpädagogischen oder psychologischen Dienstleistungen entstehen, dürfte ein standardisierter AV-Vertrag den geltenden Anforderungen prinzipiell entsprechen, vor allem den Übergang der Pflichten der Berufsgeheimnisträgerin auf die Auftragverarbeiterin betreffend. Werden die nachfolgend aufgezählten Punkte durch den Standardvertrag nicht oder nur unzureichend abgedeckt, ist ein zusätzlicher (individueller) AV-Vertrag mit der Auftragverarbeiterin zu schließen. Es empfiehlt sich, die Zusätze schriftlich zu fixieren und das von der Auftragnehmerin

gezeichnet Dokument auf dem Postweg zu verlangen, um im Falle einer Prüfung ein händig unterzeichnete Dokument vorlegen zu können.

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), ausdrücklicher *Hinweis auf den Übergang der Pflichten der Berufsgeheimnisträger*in auf die/den Auftragsverarbeiter*in*,
- Schriftlich fixierte Weisung, wie die Auftragverarbeiterin die Daten zu verarbeiten hat (Umfang der Auftragsverarbeitung, Pflichten der Auftragverarbeiterin),
- 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 die Auftragnehmerin weitere Auftragnehmerinnen im Untervertragsverhältnis einbezieht: Nachweis, dass die mit der Hauptauftragsverarbeiterin festgelegten Bedingungen auch bei den Untervertragsverarbeiterinnen[1] Anwendung finden,
- Verpflichtung der Auftragverarbeiterin, Verletzungen des Schutzes personenbezogener Daten unverzüglich anzuzeigen, sowohl gegenüber der betroffenen Person (Ratsuchende*r) wie gegenüber der Auftraggeberin,
- In diesem Zusammenhang: evtl. Benachrichtigung der zuständigen Aufsichtsbehörde (Landesdatenschützerin) durch die Auftraggeberin, wenn mit der Verletzung der Schutzrechte hohe Risiken für die Betroffenen und/oder die Auftraggeberin einhergehen[2],
- Durchführung einer Datenschutz-Folgeabschätzung durch die Auftragverarbeiterin,
- Festlegung, wie die Löschung bzw. Rückgabe der bei der Auftragverarbeiterin gespeicherten Daten nach Beendigung des AV-Vertrages erfolgt,
- Vereinbarung der Möglichkeit, die Einhaltung der geforderten Verarbeitungsprinzipien vor Ort (in den Räumen) der Auftragverarbeiterin zu prüfen ggfs. durch eine*n kundige*n Vertreter*in der Auftraggeberin prüfen und bescheinigen zu lassen.

AV-Verträge enthalten den Inhalt der Weisungen detailliert und erhalten dadurch einen gewissen Umfang[3]. Bestandteil des AV-Vertrages (Anlage) sind auch die von der Auftragverarbeiterin ausgewiesenen TOMs.

[1] Die DGOB empfiehlt, auf Untervertragsverhältnisse zu verzichten, weil sich daraus eine Reihe rechtlicher Unwägbarkeiten ergeben.
[2] Zum Beispiel bei Beratungen im Zusammenhang mit laufenden oder anstehenden Strafverfahren (Drogendelikte, Kindeswohlgefährdung etc.)

Kommt es zu einem Verstoß gegen die auferlegten Pflichten durch nachweisliches Verschulden der Auftragverarbeiterin, haftet diese für den evtl. entstandenen (und gerichtlich festgestellten) Schaden, sofern der AV-Vertrag eindeutige Regelung zum kritisierten Verstoß enthält. Der Haftungsübergang ist unbedingt im AV-Vertrag zu fixieren.

Außerdem müssen Regelungen zu folgenden Fragen getroffen werden:

- Liegen die von der Auftraggeberin erhobenen Daten bei der Auftragverarbeiterin verschlüsselt vor, so dass sie von Dritten (ohne besondere Erlaubnis[4] der Auftraggeberin) 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 bei der Auftragverarbeiterin?
- Wer hat bei der Berufsgeheimnisträgerin und bei der Auftragverarbeiterin 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?

---

[3] 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

[4] 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.

- Wie werden Datenzugriffe und Datenänderungen fälschungssicher protokolliert?
- Wenn Cloud-Dienstleister als berufsmäßig tätige Gehilfinnen 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)?
- 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 Berufsgeheimnisträgerin, 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 die berufsmäßig tätigen Gehilfinnen („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 Gehilfinnen gestellt sind (§ 203 Absatz 3 StGB).

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

Zitationshinweis:

DGOB: Datenchutz-FAQs Frage 5, 2020

Webabruf: https://dg-onlineberatung.de/wp-content/uploads/2020/04/DGOB-FAQ-5.pdf