Vorstandsmaterialien

Datenschutz – FAQ 3

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 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[1] 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[2], 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[3] 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[4], die idealer Weise nach ISO/IEC 27001 zertifiziert ist
oder
b) man greift auf zertifizierte Branchensoftware[5] zurück, die in der Regel auf einfache Weise in die bestehende Website „eingehängt“ werden kann.

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

[2] 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.

[3] 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.

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

[5] 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[6]. 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[7]. 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.

[6] 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.

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

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

Zitationshinweis:

DGOB: Datenchutz-FAQs Frage 3, 2020

Webabruf: https://