

DER DATENSCHUTZBEAUFTRAGTE FÜR KIRCHE UND DIAKONIE

Datenschutzaufsichtsbehörde
gem. Kapitel 6 DSGVO-EKD für:

Der Datenschutzbeauftragte für Kirche und Diakonie
Reichenbrander Str. 4 • 09117 Chemnitz

Ev.-Luth. Landeskirche Sachsens
Evangelische Landeskirche Anhalts
Diakonisches Werk der Ev.-Luth.
Landeskirche Sachsens e.V.
Diakonisches Werk Evangelischer
Kirchen in Mitteldeutschland e.V.

**Beauftragter für den Datenschutz
für Kirche und Diakonie**

Reichenbrander Str. 4
09117 Chemnitz

Tel.: 0351 4692-460

Fax: 0351 4692-469

Datenschutzbeauftragter@evlks.de

Kirchliche und diakonische Beratungsstellen in

- Evangelisch-Lutherische Landeskirche Sachsens
- Evangelische Landeskirche Anhalts
- Diakonisches Werk der Ev.-Luth. Landeskirche Sachsens e.V.
- Diakonisches Werk Evangelischer Kirchen in Mitteldeutschland e.V.

Aktenzeichen:

10.03.126-2023

Datum:

25.07.2023

Online-Beratungsplattform der Diakonie Deutschland

Stellungnahme des Datenschutzbeauftragten für Kirche und Diakonie als Antwort auf Fragen durch diakonische Träger und Beratungsstellen zur Möglichkeit und den Voraussetzungen des Einsatzes

Vorab

- Datenschutz ist gemäß § 1 des EKD-Datenschutzgesetzes (DSG-EKD) der Schutz jeder einzelnen Person vor Beeinträchtigungen in ihrem Persönlichkeitsrecht.

Die Vorbereitung und Durchführung von Beratungsgesprächen in kirchlichen und diakonischen Stellen ist häufig mit der Verarbeitung personenbezogener Daten der Ratsuchenden verbunden, die zu den besonderen Kategorien (§ 13 DSGVO-EKD) gehören. Sie, die Ratsuchenden, bedürfen des wirksamen Schutzes durch technische und organisatorische Maßnahmen, um die unbefugte Offenbarung der Tatsache der Beratung selbst als auch im Besonderen der (dokumentierten) Beratungs- bzw. Gesprächsinhalte zu verhindern.

Ergebnis

- Die Diakonie Deutschland Evangelisches Werk für Diakonie und Entwicklung e.V. (EWDE) stellt als Anbieter mit der Online-Beratungsplattform der Diakonie ein für die Online-Beratung technisch im Grundsatz geeignetes Mittel zur Verfügung. Dies gilt, solange nur solche Funktionen genutzt werden (können), deren prinzipiell datenschutzkonformer Einsatz durch den Hersteller ermöglicht wird. Dies ist nach unserem Kenntnisstand derzeit für die Funktionen „1:1 – Beratung“ und „Video-Call“ der Fall, wenn die Ende-zu-Ende Verschlüsselung der Kommunikationsverbindungen als auch die 2-Faktor-Authentifizierung als Pflicht für die Anmeldung der Beraterinnen und Berater an der Plattform unterbrechungsfrei aktiv und alle in der Plattform befindlichen Inhalte verschlüsselt gespeichert sind.
- Durch den Anbieter muss sichergestellt werden, dass beim Nichtfunktionieren dieser Schutzmaßnahmen als auch beim Vorliegen eines Ereignisses oder eines begründeten Verdachts, dass Dritte unbefugt durch technischen Zugriff die Kommunikation oder gespeicherten Daten auf der Plattform kompromittieren oder unzulässig verändern, Nutzer benachrichtigt und die Verbindungen

unterbrochen werden. Die einem Ereignis (z. B. Cyber-Angriff) angemessene Reaktionsfähigkeit des Supports durch den Anbieter ist mit entsprechenden Service-Level-Vereinbarungen sicherzustellen.

- **Die Eignung für den Einsatz ist damit aus datenschutzrechtlicher Sicht aber noch nicht vollständig gegeben. Durch eigene technische Vorkehrungen und organisatorische Regelungen haben Beratungsstellen ihrerseits die Möglichkeit der datenschutzkonformen Nutzung zu gewährleisten.**
- Das vom EWDE zur Verfügung gestellte „Whitepaper zu Datenschutz und Datensicherheit der Diakonie Online-Beratungsplattform“ mit Arbeitsstand vom 23.06.2023 liefert nach eigener Aussage „Basisinformationen für eine Datenschutz-Folgenabschätzung (DSFA)“, deren Durchführung, worauf das Papier hinweist, den einzelnen Rechtsträgern der Einrichtungen obliegt, die mit dem EWDE die Rahmenvereinbarung und einen Auftragsverarbeitungsvertrag abschließen.
- Die vom EWDE bereitgestellte Plattform kann eingesetzt werden, sobald die gesetzlichen Vertreter der Rechtsträger das entscheiden. Voraussetzung muss ein positives Ergebnis der DSFA und die wirksame Umsetzung der durch die DSFA empfohlenen technischen und organisatorischen Maßnahmen sein. Darüber hinaus sind alle datenschutzrechtlichen Anforderungen zu erfüllen. Die der strafbewährten Pflicht zum Schutz von Privatgeheimnissen (§ 203 StGB) unterliegenden Beraterinnen und Berater sollten in diesen Entscheidungsprozess informell einbezogen werden. Ihnen muss nach Auffassung des Datenschutzbeauftragten für Kirche und Diakonie die Nutzung der Beratungsplattform in jedem Fall freigestellt bleiben. Die Online-Beratung sollte zu keinem Zeitpunkt die Möglichkeit zur persönlichen Beratung in Präsenz in dafür geeigneten Räumen ersetzen, sondern ein zusätzliches Angebot bleiben. Damit bliebe auch den Ratsuchenden die Wahl.

Hinweise

(1) Es muss durch die Rechtsträger gewährleistet sein, dass

1. Betroffene jederzeit ihre Rechte wahrnehmen können (§§ 16-25 DSGVO_EKD) und
2. die Datenverarbeitung, egal ob digital oder auf Papier jederzeit sicher ist und die verantwortliche Stelle die Grundsätze der Verarbeitung und ihre Pflichten (§§ 5-15; 26-35 DSGVO_EKD) erfüllt.

(2) Mindestens folgende Dokumente sind zu führen:

- Verarbeitungsverzeichnis
 - Die Beratungstätigkeit muss als Verarbeitung mit den Angaben nach § 31 Abs. 1 DSGVO_EKD im Verzeichnis der Verarbeitungstätigkeiten dokumentiert sein und das im Fall der Verarbeitung von personenbezogenen Daten besonderer Kategorien unabhängig von der Anzahl der Beschäftigten (§ 31 Abs. 5 S. 2 DSGVO_EKD) beim Rechtsträger.
- DSFA-Bericht (Datenschutz-Folgenabschätzung)
 - Die DSFA hat die Anforderungen gemäß § 34 DSGVO_EKD zu berücksichtigen bzw. zu erfüllen. Das Kirchliche-Datenschutzmodell (www.kirchliches-datenschutzmodell.de) kann die Durchführung der Folgenabschätzung und Auswahl geeigneter Schutzmaßnahmen unterstützen.
 - Zur Bestätigung der Konformität der technischen Umsetzung der Online-Beratungsplattform unter Berücksichtigung von Technikgestaltung und datenschutzfreundlicher Voreinstellungen (§ 28 DSGVO_EKD) können hilfsweise Prüzfertifikate von fachkundigen und unabhängigen Dritten akzeptiert werden. Die Konformitätserklärung kann sich dabei auch auf Regelungen der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) stützen.
- Nutzungsrichtlinie
 - Die Richtlinie beinhaltet Regeln und Hinweise zur sicheren Nutzung der Online-Beratungsplattform durch Beraterinnen und Berater.

- Richtlinie zur Behandlung von Datenschutzverletzungen
 - Die Richtlinie beschreibt interne Meldewege und benennt Ansprechpartner und regelt die Zusammenarbeit mit der zuständigen Aufsichtsbehörde im Fall von Datenschutzverletzungen.
- Übersicht der Auftragsverarbeiter
 - Das EWDE ist als Auftragsverarbeiter in die Liste aufzunehmen. Die Liste kann Einträge zu den Kontrollen und Meldungen gemäß § 30 Abs. 3 S. 2 Nr. 7 u. 8 DSGVO enthalten.
- Einwilligungserklärungen
 - Soweit kein anderer Erlaubnistatbestand gemäß § 6 DSGVO oder auf Grund einer vorrangig anzuwendenden Rechtsvorschrift die Datenverarbeitung in Beratungsgesprächen erlaubt, ist eine Einwilligung nach den Anforderungen von § 11 DSGVO dokumentiert einzuholen.
- Datenschutzzinformation
 - den Ratsuchenden sind präzise, transparente und leicht verständliche Informationen gemäß § 17 DSGVO zu geben. Die Beratungsstelle erleichtert den Ratsuchenden den Zugang zu diesen Informationen, indem die Information vor dem Beginn jeder Beratung verfügbar ist und zwar mindestens in der Art und mit einem Hinweis, wo sie abrufbar ist, sodass Ratsuchende, diese bei Bedarf sofort zur Kenntnis nehmen können (§ 16 Abs. 2 DSGVO).

Die Dokumente dienen auch der Rechenschaftspflicht und sind der Aufsichtsbehörde auf Verlangen nach § 44 Abs. 1 S. 1 u. 2 i. V. m. § 5 Abs. 2 DSGVO vorzulegen bzw. Einsicht zu gewähren.

Die benannten Dokumente stellen eine Auswahl dar. Umfang und Qualität der Dokumentation zum Datenschutz muss geeignet sein das nach § 27 Abs. 1 Nr. 4 DSGVO geforderte „Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“ abzubilden.

Nachrichtlich

Informationen zur Arbeit des Datenschutzbeauftragten für Kirche und Diakonie (DSBKD) in der vorliegenden Angelegenheit mit Darstellung des Sachverhalts und dem Stand der Konsultation mit dem BfD.EKD

Ausgangspunkt für die Beschäftigung des Datenschutzbeauftragten für Kirche und Diakonie (DSBKD) mit der Online-Beratungsplattform ist die Anfrage einer Beratungsstelle, welche am 10.01.2022 durch den DSBKD entgegengenommen wurde. Seit Herbst 2022 ist auf Bitten des DSBKD der Beauftragte für den Datenschutz der EKD (BfD.EKD), als zuständige Aufsichtsbehörde für das EWDE federführend eingebunden.

Auf Grundlage einer Rahmenvereinbarung stellt das EWDE kirchlichen und diakonischen Stellen eine web- und datenbankgestützte Software in Form einer „Online-Beratungsplattform“ zur datengeschützten Kommunikation mit Ratsuchenden zur Verfügung. Auf Grundlage der Vereinbarung richtet das EWDE in der Portalanwendung Benutzerkonten ein und stellt dem Träger Ansprechpartner für die Belange der Beratungsstellen in der Online-Beratung zur

Verfügung. Ratsuchende werden auf der Webseite beratung.diakonie.de über Möglichkeiten der Kontaktaufnahme informiert, wobei dort auch Beratungsstellen verzeichnet werden, die keine oder andere Lösungen als die Online-Beratungsplattform einsetzen.

Jeder Rechtsträger hat gemäß den Vereinbarungen zu gewährleisten, dass Beraterinnen und Berater die notwendigen technischen und fachlichen Schulungen zur Durchführung der Online-Beratung erhalten. Im Vertrag regelt das EWDE, dass Träger den Schutz der vertraulichen Daten innerhalb der Dienststelle gemäß Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD) zu gewährleisten haben. Der Träger hat auch dafür zu sorgen, dass Mitarbeiter der Beratungsstellen, die ein Benutzerkonto bedienen, die Vertraulichkeit sowie die Qualität der verwendeten Passwörter gewährleisten und das EWDE umgehend über

jeden unberechtigten Zugriff informiert wird (Diese Meldung muss anonymisiert erfolgen, Anm. Red.).

Zusammen mit der Rahmenvereinbarung schließen Träger einen Auftragsverarbeitungsvertrag (AVV) ab. Damit erklärt der Rechtsträger, dass jede Nutzung der Plattformanwendung eine von ihm erteilte Weisung ist (§ 30 Abs. 4 Satz 1 DSGVO) und die datenschutzrechtliche Verantwortung dem Rechtsträger als Auftraggeber allein obliegt.

Auch nach der letzten Konsultation zwischen den beteiligten evangelischen Aufsichtsbehörden im Juni 2023 kann ein Ausräumen aller datenschutzrechtlichen Bedenken seitens der Aufsichtsbehörden zum jetzigen Zeitpunkt noch nicht bestätigt werden. An dieser Stelle ist zu wiederholen, dass Datenschutzaufsichtsbehörden nicht die Aufgabe haben, positive oder negative Produktempfehlungen abzugeben. Es bleibt in der alleinigen Verantwortung jeder Stelle, den Einsatz solcher Werkzeuge für die eigene Praxis zu entscheiden. Dies betonte zuletzt auch der Vorstand des Diakonischen Werkes der Ev.-Luth. Landeskirche Sachsens, als er die Nutzung der Online-Beratungsplattform dem Grundsatz nach allen Mitgliedseinrichtungen empfahl.

Fortlaufend sind der BfD.EKD und der DSBKD zur Online-Beratungsplattform Konsultation. Wegen der gleichen Technik der Plattformanwendung für die Diakonie als auch für die Caritas informieren sich die Aufsichtsbehörden in der EKD und die zuständige katholische Aufsichtsbehörde über ihre Arbeit zum Thema.

Wenn auch juristisch nicht zu beanstanden, ist die Vertragskonstruktion mit einer Vereinbarung zur Auftragsverarbeitung aus Sicht des DSBKD nicht die für kleine und mittlere Rechtsträger beste Form, weil dadurch jede einzelne Beratungsstelle bzw. jeder Rechtsträger allein die datenschutzrechtliche Verantwortung und den damit verbundenen Aufwand zu tragen hat. Dem Sinn eines Dienstes der Diakonie Deutschland für angeschlossene Werke und Mitgliedseinrichtungen entspräche, wenn das EWDE die Verantwortung für eine sichere Bereitstellung dergestalt übernehme, dass sie den Rechtsträgern einen Vertrag über die gemeinsame Verantwortung gemäß § 29 DSGVO anböte oder die Datenschutzkonformität durch unabhängige Dritte zertifizieren ließe.

Wenn die nach § 34 DSGVO bestehende Pflicht zur Datenschutz-Folgenabschätzung kleine oder mittlere Beratungsstellen bzw. ihre Träger überfordert, könnten diese als Konsequenz die Beratungsplattform nicht einsetzen.

Im Blick darauf ist es opportun zu fragen, ob es nicht hilfreich sein kann, wenn Landesverbände gemeinsam mit oder interessierte Mitglieder untereinander eine einheitliche Vorgehensweise in der Online-Beratung unter Nutzung der Online-Beratungsplattform beschreiben und die Schutzmaßnahmen nebst den Dokumenten in ihren Organisationen in gleicher Weise umsetzen. Der Datenschutzbeauftragte für Kirche und Diakonie würde dabei im Rahmen seiner Möglichkeiten beratend unterstützen.

Chemnitz, am 25.07.2023

Der Datenschutzbeauftragte für Kirche und Diakonie
Datenschutzaufsichtsbehörde nach Kapitel 6 EKD-Datenschutzgesetz für
die Evangelisch-Lutherische Landeskirche Sachsens
die Evangelische Landeskirche Anhalts
das Diakonische Werk der Evangelisch-Lutherischen Landeskirche Sachsens e.V.
das Diakonische Werk Evangelischer Kirchen in Mitteldeutschland e.V.