Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Stand: 29.04.2020

Datenschutzanforderungen an Online-Beratungsangebote[1]

Beratungsangebote, teilweise auch in sensiblen Bereichen, werden vielfach und verstärkt derzeit vor dem Hintergrund der Coronavirus-Pandemie nicht mehr nur vor Ort oder per Telefon, sondern zusätzlich auch online durch rein textliche Kommunikation angeboten. Ziel ist es, ein möglichst niederschwelliges Angebot zu ermöglichen. Das Angebot holt die Beratungssuchenden idealerweise in denjenigen digitalen Medien ab, in denen sie sich regelmäßig bewegen. Die Hemmschwellen für eine persönliche Kontaktaufnahme sollen auf diese Weise verringert werden.

Da die Beratung normalerweise vertraulich erfolgen soll, sind aus datenschutzrechtlicher Sicht die folgenden Aspekte unbedingt zu beachten:

1. Die mit dem Angebot einhergehende Datenverarbeitung muss den Beratungssuchenden transparent und nachvollziehbar dargestellt werden. Hierzu gehört, dass deutlich wird, für welche Zwecke und durch wen Daten (Inhaltsdaten wie z. B. Fragen und Antworten, IP-Adressen und Metadaten wie Zeitpunkte, Cookies, Nutzernamen etc.) verarbeitet werden und wie lange welche Daten gespeichert bleiben. Die Anbieter entsprechender Angebote sind verpflichtet, ihren Informationspflichten nach Art. 12 ff. DS-GVO nachzukommen.

2. Die Beratung darf keinesfalls innerhalb von Online-Angeboten erfolgen, deren Geschäftsmodell auch die Auswertung personenbezogener Daten der Nutzenden ist. Beispiele hierfür sind die werbefinanzierten Kommunikationsdienste von Facebook oder Google.

3. Um eine anonyme oder pseudonyme Beratung zu ermöglichen, darf diese nicht über Plattformen oder Dienste erfolgen, die eine Anmeldung mit identifizierenden Daten verlangen.

4. Beratungen per Messenger-Dienst, SMS oder auch E-Mail sind daher i. d. R. nicht möglich. Ausnahmen könnten ggf. Messenger-Dienste bieten, die unabhängig von Identitätsdaten wie Telefonnummer oder E-Mail arbeiten. Informationen dazu finden sich im Beitrag zum datenschutzgerechten Einsatz von Messenger-Diensten im aktuellen Jahresbericht der Berliner Beauftragten für Datenschutz und Informationsfreiheit[2].

[1] In unserem Jahresbericht 2017 haben wir über ein von unserer Behörde datenschutzrechtlich begleitetes Projekt für ein Online-Beratungsangebot im Kinder- und Jugendhilfebereich berichtet (Abschnitt 6.2, S. 84 ff.). Die an entsprechende Beratungsangebote zu stellenden Anforderungen haben wir in einem Merkblatt zusammengefasst, um auch anderen Beratungsdiensten zu helfen, ihre Angebote von vornherein datenschutzgerecht zu gestalten. Wir haben die aktuelle Situation zum Anlass genommen, das Merkblatt zu aktualisieren und an die aktuelle Rechtslage, insbesondere der Datenschutz-Grundverordnung, anzupassen.

[2] Jahresbericht 2019, Abschnitt 1.1, S. 17ff., abrufbar unter: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2019-Web.pdf

Internet: https://www.datenschutz-berlin.de
E-Mail: mailbox@datenschutz-berlin.de
Friedrichstr. 219
10969 Berlin
Tel: (030) 13889 - 0
Fax: (030) 13889 201

5. Einer Beratung per E-Mail steht zudem entgegen, dass nicht einmal die Grundanforderung an die vertrauliche Übermittlung personenbezogener Daten sichergestellt werden kann, wenn die Übertragung ohne Ende-zu-Ende-Verschlüsselung erfolgt.

6. Wird eine anonyme Beratung versprochen, dürfen nur die für den Betrieb des Beratungsangebotes technisch unbedingt erforderlichen identifizierenden Daten erhoben und für den kürzest notwendigen Zeitraum gespeichert werden. Sowohl für die Inhaltsdaten als auch für die Nutzungsdaten ist ein Löschkonzept zu entwickeln und die Notwendigkeit der darin festgelegten Speicherdauer zu begründen.

7. Die Verarbeitung von IP-Adressen ist nur innerhalb der jeweiligen Sitzung des Nutzenden technisch notwendig. Eine vorsorgliche Speicherung von personenbezogenen Daten wie beispielsweise der IP-Adresse lässt die Anonymität des Beratungsangebotes entfallen. Eine vorsorgliche Speicherung mit dem Ziel, die verbindlich zugesagte Anonymität in bestimmten Fällen, z. B. für Zwecke der Gefahrenabwehr, zu brechen, ist nicht zulässig.

8. Der Einsatz von Dritt-Inhalten, insbesondere externen Tracking- und Analysefunktionen sowie die Einbindung von Social-Plug-Ins, d. h. Funktionen, über die die Inhalte des Angebots mit sozialen Netzwerken geteilt werden können, sind auf Webseiten von Beratungsangeboten nicht zulässig. Ansonsten würden bereits bei Aufruf der Webseite unzulässig personenbezogene Daten an Dritte übermittelt oder von diesen erhoben werden.

9. Online-Beratungsangebote müssen so gestaltet werden, dass ein hohes Niveau an IT-Sicherheit erreicht wird. Trotz eines vornehmlich anonymen Beratungsangebots ist eine zumindest temporäre Verarbeitung identifizierender Daten, wie z. B. IP-Adressen, identifizierende Angaben in den Nachrichten der Beratungssuchenden, bei manchen Plattformen auch freiwillig angegebene E-Mail-Adressen, nicht völlig vermeidbar. Da bei der Erbringung von Beratungsangeboten häufig auch besonders sensitive Daten im Sinne des Art. 9 Abs. 1 der Datenschutz-Grundverordnung (DS-GVO) wie beispielsweise Gesundheitsdaten, Daten zum Sexualleben oder auch über die ethnische Herkunft verarbeitet werden, sind IT-Sicherheitsmaßnahmen zu treffen, die bezüglich des Schutzziels der Vertraulichkeit möglichst das Schutzniveau „hoch“ entsprechend BSI-IT-Grundschutz erreichen.

Weitere Erläuterungen zu einigen der vorherigen Punkte:

Einsatz sozialer Netzwerke (Punkt 2)

Oft wird von Beratungsanbietern argumentiert, dass insbesondere Jugendliche nur noch in sozialen Netzwerken oder ähnlichen Angeboten – meist US-amerikanischer Konzerne – zu erreichen seien. Allerdings ist an dieser Stelle klarzustellen, dass eine Beratung nicht direkt in dem jeweiligen Netzwerk erfolgen kann, da hierbei die Vertraulichkeit gegenüber dem Beratungssuchenden verletzt würde. Insbesondere werbefinanzierte Angebote werten die Aktivitäten ihrer Nutzerinnen und Nutzer umfassend aus und versuchen, die entsprechenden Algorithmen immer weiter zu verbessern, die aus den Beobachtungen Persönlichkeitsprofile auch und insbesondere über sensible Aspekte erstellen.

Aus diesem Grund ist Vorsicht geboten, wenn Beratungsangebote lediglich Informationsseiten in entsprechenden sozialen Netzwerken anbieten. Es besteht immer die Gefahr, dass Plattformbetreiber aus dem reinen Besuch einer Informationsseite im sozialen Netzwerk zu einem externen

Beratungsangebot oder gar der Interaktion des Betroffenen mit diesem Informationsangebot Rückschlüsse über sensible Informationen zu der Person oder zu bestehenden Problemen ziehen.

Technische Konzeptionen von Beratungsangeboten (Punkte 3 - 5)

Konzeptionell können Beratungsangebote unproblematisch realisiert werden, bei denen Betroffene in Echtzeit mit Beratern chatten oder telefonieren. Hierbei ist grundsätzlich keine Anmeldung des zu Beratenden und damit abgesehen von den anfallenden Nutzungsdaten (z. B. der IP-Adresse) keine Angabe von personenbezogenen Daten erforderlich.

Problematischer sind asynchrone Beratungsangebote, die technisch ähnlich wie E-Mails auf einem Austausch und dem Zwischenspeichern von Nachrichten basieren. Hierfür werden meist Portal-Lösungen genutzt, in denen die Beratungssuchenden einen Account unter einem Pseudonym erstellen, ihre Fragen hinterlassen und später die Antworten abrufen können.

Eine solche Lösung würde konzeptionell die Anforderungen an eine anonyme Beratung erfüllen, wenn das Portal technisch mit ausreichend hohen IT-Sicherheitsmaßnahmen umgesetzt wird. Allerdings ist der Diensteanbieter verpflichtet, die Nutzenden in seiner Datenschutzerklärung darauf hinzuweisen, dass es sich formal um ein Beratungsangebot unter Pseudonym handelt, da durch den Account eine Wiedererkennung der Beratungssuchenden möglich und notwendig ist.

Sollte in dem Beratungsangebot die Möglichkeit bestehen, eine E-Mail-Adresse anzugeben, um die Beratungssuchenden über eine Antwort zu benachrichtigen, so ist deutlich darauf hinzuweisen, dass die Angabe der E-Mail-Adresse für die Inanspruchnahme dieser Benachrichtigungsfunktion keinesfalls notwendig ist, um das Beratungsangebot generell in Anspruch nehmen zu können. Auch sind die Beratungssuchenden darüber zu informieren, dass die E-Mail-Adresse nur zur technischen Realisierung der Benachrichtigung genutzt wird, jedoch von den Beratern nicht eingesehen werden kann. Zudem sollte den Nutzenden empfohlen werden, E-Mail-Adressen zu verwenden, die keine Rückschlüsse auf ihren Namen zulassen (z. B. anstelle von max.müller@example.com besser x1725406@example.com) – also beispielsweise eine eigens hierfür eingerichtete E-Mail zu nutzen.

Anonymitätsversprechen muss eingehalten werden (Punkte 6 und 7)

Online-Beratungsangebote richten sich oftmals an Beratungssuchende, die ein solches Angebot auf Grund ihrer persönlichen Situation nur deswegen in Anspruch nehmen, weil sie sich von der Online-Beratung die Wahrung größtmöglicher Anonymität erhoffen. Gegenüber der Inanspruchnahme einer persönlichen „Face-to-Face-Beratung“ sind entsprechende Angebote niederschwelliger.

Jede Form der Beratung von Menschen in schwierigen Lebenssituationen setzt Vertrauen voraus. Vertrauen bildet die Basis einer erfolgreichen Hilfe. Dem nachvollziehbaren Wunsch nach Vertraulichkeit und größtmöglicher Anonymität muss bereits bei der Ausgestaltung derartiger Angebote Rechnung getragen werden. Dazu gehört, dass die Erhebung und Speicherung personenbezogener Daten auf ein Mindestmaß reduziert wird. Konkret bedeutet dies, dass identifizierende Angaben über den Nutzer (dazu gehört auch die IP-Adresse) nur verarbeitet werden dürfen, soweit dies zwingend für die Erbringung des Dienstes notwendig ist. Eine Speicherung von IP-Ad-

ressen im Sinne einer Vorratsdatenspeicherung etwa für den Fall, dass diese ggf. später für Zwecke der Gefahrenabwehr oder ein strafrechtliches Ermittlungsverfahren benötigt werden könnten, ist unzulässig und gesetzlich gerade nicht vorgesehen.

Mindestens notwendige IT-Sicherheitsmaßnahmen (Punkt 9)

Um ein angemessenes IT-Sicherheitsniveau sicherzustellen, ist es erforderlich, zunächst eine Risikobewertung vorzunehmen. Sodann sind die technischen und organisatorischen Maßnahmen umzusetzen, die erforderlich sind, um die Rechte der Betroffenen zu wahren. Hierzu gehört auch die Erstellung eines IT-Sicherheitskonzepts. Dieses sollte auf Basis einer anerkannten Methode, wie z. B. des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI), erfolgen, ergänzt um zusätzliche Maßnahmen zur Erreichung eines hohen Schutzniveaus. Für öffentliche Angebote des Landes Berlin verpflichtet § 26 Abs. 2 Berliner Datenschutzgesetz (BlnDSG) die Anbieter, die zu ergreifenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse zu ermitteln und in einem Datenschutzkonzept zu dokumentieren. Je nach Sensitivität und Menge der voraussichtlich zu verarbeitenden personenbezogenen Daten kann auch die Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO erforderlich sein. Das IT-Sicherheitskonzept, das Datenschutzkonzept sowie die Datenschutz-Folgenabschätzung können in einem Dokument niedergelegt werden, da die Risikoanalyse üblicherweise Bestandteil aller drei Dokumente ist.

Mindestens erforderlich sind nach derzeitigem Stand folgende Maßnahmen:

- Verschlüsselung der Verbindung zwischen Web-Angebot und Client mit den jeweils dem Stand der Technik entsprechenden kryptographischen Verfahren und Schlüssellängen (z. B. Verbindungsaufbau nur über https, nicht aber mit http, TLS mindestens Version 1.2, keine Unterstützung von SSL und unsicheren Chiffren).

- Einsatz einer Methode zur Mehrfaktor-Authentifizierung für Personen wie Berater oder Administratoren, die auf den Nachrichtenverlauf mehrerer Personen zugreifen oder entsprechende Zugriffsberechtigungen einsetzen bzw. manipulieren können.

- Die Server müssen entweder selbst betrieben werden oder es ist ein zuverlässiger Dienstleister mit Firmensitz und Datenverarbeitung innerhalb der Europäischen Union einzusetzen. In der zweiten Variante ist zudem der Abschluss eines Auftragsverarbeitungsvertrages erforderlich, welcher den Anforderungen des Art. 28 DS-GVO entspricht.

- Kontrolle des Datenverkehrs mit dem Internet durch restriktiv konfigurierte Firewalls.

- Logische Trennung von Web-Frontend und Backend der Serveranwendung.

- Die Einbindung von Inhalten Dritter wie z. B. Fonts, Scripte oder gar Trackingdienste muss im gesamten Angebot unterbleiben. Theoretisch wäre zwar in Einzelfällen eine Einbindung denkbar, faktisch lassen sich die hohen rechtlichen Anforderungen jedoch üblicherweise

nicht erfüllen.[3] Es ist zu verhindern, dass personenbezogene Daten an diese Dritten übermittelt werden. Bereits die Information, dass die hinter einer bestimmten IP-Adresse stehenden Personen das Beratungsangebot nutzen, ist schützenswert. Dies gilt insbesondere vor dem Hintergrund, dass großen Anbietern die Identifizierung der jeweiligen zu beratenden Person z. B. anhand der IP-Adresse aufgrund anderer Nutzungen von deren Diensten oft technisch möglich ist.

[3] Es sind die Anforderungen der Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien (Stand: März 2019), herausgegeben durch die Konferenz der unabhängigen Aufsichtsbehörden des Bundes und der Länder (abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf) zu beachten.