e-beratungsjournal.net
Fachzeitschrift für Onlineberatung und computervermittelte Kommunikation
ISSN 1816 - 7632

13. Jahrgang, Heft 2, Artikel 1
2017

Auf der sicheren Seite
Standards zum Datenschutz der bke-Onlineberatung

Corinna Gekeler

Zusammenfassung
Der Schutz der Persönlichkeitsrechte Ratsuchender gehört zum Selbstverständnis von Beratungsangeboten und ist Ziel des Bundesdatenschutzgesetzes (BDSG). Am Praxisbeispiel der beiden Portale der Onlineberatung der bke (Bundeskonferenz für Erziehungsberatung e.V.) werden Grundsätze, technisch-organisatorische Maßnahmen und gesetzliche Vorgaben zum Datenschutz besprochen. Der Beitrag geht auf die Besonderheiten der Schweigepflicht ein, auf reale Risiken und auf die europäische Datenschutz-Grundverordnung (DSGVO), die das BDSG im Mai 2018 quasi ablösen wird.

Schlüsselwörter
Datenschutz, Datensicherheit, Online-Beratung, Schweigepflicht, Berufsgeheimnis, Persönlichkeitsrechte, Technisch-organisatorische Maßnahmen, Bundesdatenschutzgesetz (BDSG), Europäische Datenschutz-Grundverordnung (DSGVO)

Abstract
Protecting the personal rights of the persons seeking for online consult is part of the self-concept of online helpdesks. This protection is as well the target of the German Federal Data Privacy and Protection Act. Along the practical example of the online-helpdesks for young persons and for parents offered by the bke (Bundeskonferenz für Erziehungsberatung e.V.) this article discusses basic principles, technical and organisational measures and legal guidelines for data and privacy protection. It deepens the specifics of professional secrecy, the real risks for the data and the European General Data Protection Regulation (GDPR) which will more or less replace the recent data protection laws in May 2018.

Keywords
Data Privacy, Data Protection, Online Consultation, Professional Secrecy, Personal Rights, Technical-organisational Measures, German Federal Data Privacy and Protection Act, General Data Protection Regulation (GDPR)

Autorin
- **Corinna Gekeler**
- zertifizierte Fachkraft für Datenschutz
- Politikwissenschaftlerin
- Publizistin mit den Schwerpunkten Grundrechte, Diskriminierungsschutz und Selfempowerment
- Medienpreisträgerin der Deutschen AIDS-Stiftung
- Externe Datenschutzbeauftragte der Bundeskonferenz für Erziehungsberatung (bke)
- Seminare „Datenschutz in der Beratung" (u.a. AWO Bundesakademie)
- Betreuung des Datenschutzes der Onlineberatung der Deutschen AIDS-Hilfe (aidshilfe-beratung.de) von Beginn an.
- **Kontakt:** Web: http://www.wellenlaengen-beratung.de

1. Einleitung

Der Begriff Datenschutz löst bei vielen Beschäftigten im Gesundheits- und Sozialbereich erst einmal Gefühle der Unsicherheit und Widerstände gegen Technik aus. Und zwar obwohl Datenschutz gerade in der Online-Beratung im Sozial- und Gesundheitsbereich eine Voraussetzung für deren vertrauliche Umsetzung ist.

Geht man vom Recht auf ein selbstbestimmtes Leben aus, sind die Persönlichkeitsrechte des Gegenübers entsprechend zu respektieren und zu schützen. Datenschutz betrifft also bei Weitem nicht nur die technischen Rahmenbedingungen, sondern berührt zentrale Fragen der Haltung gegenüber den Ratsuchenden und somit auch zum Umgang mit ihren Daten. Außerdem ist Schweigepflicht eine zentrale Säule in der Erziehungsberatung und Datenschutz eine der sogenannten beruflichen Nebenpflichten.

Dieser Beitrag erläutert Grundlagen zum Datenschutz am Praxisbeispiel der Onlineberatungsportale der Bundeskonferenz für Erziehungsberatung (bke) für Eltern (https://eltern.bke-beratung.de/views/home/index.html) und für Jugendliche (https://jugend.bke-beratung.de/views/home/index.html). Er basiert auf einem Beitrag im bke-Jahresbericht 2016 (http://bke.de/content/application/explorer/public/virtuelle-beratungsstelle/bke-online-bericht-2016-web.pdf). Die Ausführungen zu rechtlichen Rahmenbedingungen beziehen sich auf die Situation in Deutschland.

2. Grundrecht

Das Selbstverständnis vieler Beratungsstellen kommt dem Ansatz der Gesetzgebung zum Datenschutz recht nah. Beide setzen sich für den Schutz von Persönlichkeitsrechten ein, sogar das Wort Selbstbestimmung nutzen viele Beratungsangebote ebenso wie der Gesetzgeber. Im Bundesdatenschutzgesetz (BDSG) steht das Recht auf informationelle Selbstbestimmung an erster Stelle. Es handelt sich sogar um ein Grundrecht aller Bürgerinnen und Bürger auf einen Umgang mit ihren Daten nach ihren Wünschen und Bedarfen.

Die Rechtslage ist eindeutig und bedeutet für die beiden Online-Portale der bke Folgendes: Den Ratsuchenden gehören alle über sie gespeicherten Daten, die nur mit ihrer Einwilligung erfasst und bearbeitet oder gar weitergeleitet werden dürfen. Anbieter müssen vorweg darüber informieren, zu welchem Zweck ihre Daten erfasst werden. Die gebotene Transparenz beinhaltet auch eine umfassende Aufklärung über den weiteren Umgang mit den „Kundendaten", also Informationen darüber, wo und unter welchen Vorsichtmaßnahmen die Daten gespeichert werden und wer sie einsehen und gegebenenfalls löschen darf. So steht jeder Anbieter von Online-Portalen vor der Herausforderung, den Ratsuchenden möglichst verständliche Erläuterungen in seinen Nutzungsbedingungen und seiner Datenschutzerklärung zu bieten.

Bevor die Nutzer/innen über die Datenschutz-Standards informiert werden können, muss jedoch erst eine sogenannte Datenschutz-Organisation stattfinden, die dem Selbstverständnis des jeweiligen Angebots und den gesetzlichen Vorgaben gleichermaßen entspricht. Die Rahmenbedingungen zum Datenschutz einer Online-Beratung müssen nach folgenden Gesetzen gestaltet werden:

- Das Bundesdatenschutzgesetz (BDSG), das im Mai 2018 von der Europäischen Datenschutz-Grundverordnung (EU-DS-GVO) abgelöst wird.
- Als Betreiber eines Online-Angebotes muss die bke das Telemediengesetz (TMG) beachten.
- Das Telekommunikationsgesetz (TKG) spielt eine Rolle, da Kommunikationsdaten anfallen.
- Die Mitarbeitenden unterliegen der Schweigepflicht (§203 StGB).
- Das Strafgesetzbuch (StGB) regelt, unter welchen Umständen eine Durchbrechung der Schweigepflicht geboten oder verboten ist.

3. „Tür zu!"

Der Begriff Vertraulichkeit beschreibt das Verhältnis zwischen Ratsuchenden und Berater/innen am treffendsten. Im Setting einer Beratungsstelle wird dieses hohe Gut ganz selbstverständlich durch das Schließen der Tür des Beratungsraums ermöglicht, damit keine andere Person Zugang zum Gesprochenen hat. Genauso wie man nicht auf einem belebten Marktplatz lautstark eine Beratung durchführen würde, müssen entsprechende Schutzräume für die virtuelle Beratung geschaffen werden. Und da es nicht vorstellbar ist, eine Beratung per Postkarte durchzuführen, können auch keine gewöhnlichen E-Mails dafür verwendet werden, da dies einer untersagten Offenbarung von Geheimnissen entsprechen würde.

Doch wie lässt sich eine angemessene Vertraulichkeit auf das Setting der bke-Onlineberatung übertragen? Ist ein „Tür zu!" hier überhaupt möglich, wo doch jeder Schritt im Internet Datenspuren hinterlässt, die leicht in Hände Unbefugter gelangen können?

Laut BDSG handelt es sich bei der bke-Onlineberatung um besonders schützenswerte Daten, da meist sensible Bereiche wie Gesundheit oder etwa Sexualität berührt sind. Demnach wird auch ein entsprechend hohes Schutzniveau erwartet. Doch welche Maßnahmen hat die bke für ihre beiden Beratungsportale (https://jugend.bke-beratung.de und https://eltern.bke-beratung.de) ergriffen? Von der technischen Seite ermöglichen die beiden Beratungsportale durch folgende Software-Lösungen eine gut gesicherte Kommunikation:

- Alle Beratungsvorgänge finden nur auf einem besonders gesicherten Server statt (webbasiert) und liegen nicht auf Computern in den teilnehmenden Beratungsstellen oder der bke. Ein solcher zentraler Speicherplatz erspart auch das Hin- und Hersenden der heiklen Daten.
- Wer sich in die Beratungssoftware mithilfe von Benutzername und Passwort einloggt, gelangt nur auf einem verschlüsselten Weg an seine Daten (SSL-Verschlüsselung). Im Browser ist dies daran zu erkennen, dass dort ein „https" statt einem „http" steht.

- Weder das Beratungsteam noch die Administrator/innen der Portale sehen die IP-Adressen mit denen Ratsuchende im Internet unterwegs sind. Auch die E-Mail-Adressen, die Ratsuchende hinterlegen können, um Benachrichtigungen zu erhalten, sind nicht einsehbar. Nur so kann von einer anonymen Beratung die Rede sein.

Über die Software hinaus wird eine möglichst hohe Datensparsamkeit erzielt. Das BDSG schreibt vor, dass nur genau die Daten erfasst werden dürfen, die für die Durchführung einer fachlich guten Beratungsarbeit nötig sind. Das fängt damit an, dass nur wenige Anhaltspunkte in der Anmeldemaske abgefragt werden und gilt selbstverständlich auch für die Berater/innen, die sich keinesfalls ein umfassendes Bild machen, sondern sich in ihren sparsam dosierten Nachfragen auf fachlich gebotene Merkmale der Umstände beschränken.

Außerdem geben Ratsuchende beim Benutzernamen nicht ihren richtigen Namen an, sondern nur sogenannte Nicknamen, wodurch die Beratung pseudonymisiert stattfindet. Auch wenn Ratsuchende aufschlussreiche Details zu ihrer Person offenlegen, sind die Berater/innen verpflichtet, diese für sich zu behalten.

Im Normalbetrieb wird also niemand bei den Beratungen mitlesen. Lediglich in begründeten Ausnahmefällen, zum Beispiel wenn eine Beschwerde gegen den bzw. die Berater/in oder den bzw. die User/in vorliegt, kann die fachliche Leitung der bke-Onlineberatung Einblick in die betreffenden Beratungsvorgänge nehmen. Davon werden alle Betroffenen umgehend informiert.

Des Weiteren kann die fachliche Leitung zur Einhaltung der fachlichen Standards in Abstimmung mit der bzw. dem jeweiligen Berater/in Einsicht in bestimmte Beratungen nehmen. Eine weitere Maßnahme zur Qualitätssicherung stellt der kollegiale Austausch im Beraterteam und in der Supervision dar. Dieser findet selbstverständlich nur im geschützten Raum der Beratungssoftware und anhand von Daten ohne Personenbezug (also pseudonym) statt.

Zur Umsetzung der Onlineberatung ist die bke natürlich auf Dienstleister im Bereich der Beratungssoftware und des Server-Hostings angewiesen. Deren Umgang mit den Daten und deren Datenschutz-Maßnahmen werden in sogenannten ADV-Verträgen genau geregelt, wobei ADV für Auftragsdaten-verarbeitung steht.

4. Glieder einer Kette

Datenschutz-Standards und andere Qualitätsmerkmale funktionieren nur, wenn sie an allen entscheidenden Stellen konsequent umgesetzt werden können. Wie bei den Gliedern einer Kette gilt hier auch, dass das schwächste Glied zum Problem werden kann. Wie so oft ist das auch beim Datenschutz meist der Mensch, der unwissend, fahrlässig oder einfach nur bequem handelt. Eine weitere „Schwachstelle" sind Geräte und Internetverbindungen, von denen aus die Beratung stattfindet und für die deshalb von der bke Auflagen zur Sicherheit entwickelt wurden.

Alle Mitarbeitenden der bke-Onlineberatung unterliegen der Schweigepflicht und müssen einen von der bke speziell entwickelten Leitfaden zum Datenschutz einhalten. Zu diesen Datenschutzstandards erhalten neue Berater/innen im Rahmen der bke-Fortbildung und alle Mitarbeitenden auf der jährlichen Klausurtagung eine Schulung. So weiß jede/r, was er bzw. sie beitragen kann, um auch in der bke-Onlineberatung „die Tür zuzumachen".

Datenschutz gelingt am besten, wenn bei den Standards ein Mittelweg gefunden wird, der die Nutzerfreundlichkeit der Beratungs-Software, die sogenannte Usability, nicht einschränkt. Das heißt, der Aufwand muss nachvollziehbar sein und im Bereich der Verhältnismäßigkeit und der Machbarkeit liegen. Nur so gelingen praxisnahe Lösungen, die möglichst konsequent umgesetzt werden.

Auf der Seite der Ratsuchenden bedeuten die Datenschutz-Maßnahmen der bke, dass es keine Beratung per App mehr gibt und dass die Ratsuchenden nach einiger Zeit der Inaktivität automatisch ausgeloggt werden.

Für das Beraterteam gibt es bestimmte Regeln, von wo aus man sich in die Beratungssoftware einloggen darf. Dies ist nur von einem eigenen Benutzerkonto auf dem PC aus möglich und selbstverständlich darf das Passwort niemals Anderen bekannt werden. Der Datenschutz geht aber auch mit Einschränkungen einher. So dürfen zum Beispiel Beratungsvorgänge nicht auf den eigenen Computer kopiert werden. Auch ein Login auf mobilen Endgeräten (Laptops usw.) unterliegt strengen Auflagen. Die Nutzung von WLAN-Verbindungen ist nur eingeschränkt zugelassen und ein Login auf einem Smartphone ist nicht gestattet.

Die Bereitstellung entsprechend geschützter Geräte und Verbindungen sowie die Einhaltung der Standards durch die Berater/innen liegt in der Verantwortung der Beratungsstellen vor Ort. Sie sind die direkten Arbeitgeber der beratenden Fachkräfte und gehen als solche eine Kooperation mit der bke ein, die den Rahmen für die Zusammenarbeit in einem Kooperationsvertrag vorgibt. In der Verantwortung der bke liegt es, für die Beratungssoftware, Schulungen, Datenschutz-Standards und für die fachliche Betreuung und Weiterentwicklung sowie die Bewerbung der beiden Beratungsportale zu sorgen.

5. Reale Risiken

Beim Datenschutz sollte es nicht um den Aufbau von Drohszenarien gehen, aber die realen Risiken müssen verständlich gemacht werden. Dazu gehört das Wissen darüber, dass in unserem digitalen Zeitalter Daten das „neue Gold" sind. Die Beratungsvorgänge stellen demnach einen Schatz dar, den es zu schützen gilt. Deshalb ist es notwendig, dass dieser Schatz durch einen Datentunnel (SSL) geschützt wird und die Daten die Beratungssoftware nicht verlassen (webbasierte Mailberatung).

„Was soll schon passieren?" und „wer interessiert sich schon für unsere Daten?" mag man sich fragen. Den Wert der Daten im illegalen Datenhandel real einzuschätzen, ist schwierig. Da es sich aber für die meisten potenziell Betroffenen um wirklich heikle Informationen handelt, dürfte das den Preis steigern. Meist sind die, die sich über technische Tricks illegalen Zugang verschaffen, nur Lieferanten,

die mit ihrer Beute zum Hehler (Datenhändler) gehen. Weniger kriminelle Motive können eine Art Voyeurismus sein oder die Ambitionen und Konkurrenzkämpfe technisch versierter Jugendlicher. Aber auch diese können Schaden anrichten.

6. Ausnahmen

Wie bei allen Regeln gibt es auch beim Datenschutz Ausnahmen. So dürfen bzw. müssen in genau definierten Ausnahmesituationen sogar Daten mit Personenbezug eingesehen oder weitergegeben werden. Für die unterschiedlichen Eventualitäten hat die bke exakt festgelegte Abläufe definiert, nach denen im Bedarfsfall zu handeln ist.

Zum Schutz der Portale
Der Server mit allen Vorgängen der bke-Onlineberatung wird von einer Hosting-Firma bereitgestellt, mit der ein Vertrag über alle Details zu Datenschutz und Datensicherheit abgeschlossen wurde. Datensicherheit meint den Schutz vor Verlust oder Manipulation von Daten und die Abwehr von Hackerangriffen. Um ein hohes Niveau an Datensicherheit gewährleisten und eventuelle Angriffe abwehren zu können, darf die Server-Firma die Verbindungsdaten (IP-Adressen, Login-Zeit usw.) eine Woche lang speichern. Und zwar einzig zu diesem Zweck.

Zum Schutz der Ratsuchenden
Das Strafgesetzbuch (StGB) regelt den Schutz der Privatgeheimnisse der Ratsuchenden in zweierlei Hinsicht:

- Alle Mitarbeitenden der bke-Onlineberatung fallen unter die berufliche Schweigepflicht nach §203 StGB. Wenn sie Geheimnisse unbefugt offenbaren, können sie mit einer Freiheitsstrafe bis zu einem Jahr, bei bestimmten Beweggründen sogar bis zu zwei Jahren, bestraft werden.
- Wenn es um das durch Suizid bedrohte Leben eines/einer Ratsuchenden geht, verpflichtet das StGB zur Offenbarung der Daten. Bei einer deutlich geäußerten Ankündigung einer Suizidabsicht gebietet §323c StGB (Unterlassene Hilfeleistung) eine Durchbrechung der Schweigepflicht, um die Gefahr abzuwenden. Was es bei der fachlichen Beurteilung einer solchen Situation zu beachten gilt, hat die bke ausführlich für das Beraterteam erarbeitet.

Zum Schutz der Allgemeinheit und des Lebens Dritter
Ankündigungen einer schweren Straftat müssen nach §138 StGB angezeigt werden. Wer glaubhaft von konkreten Plänen oder bereits begonnenen Taten bezüglich Mord, Geiselnahme, Terrorangriff, Amoklauf o.ä. erfährt, muss die Ermittlungsbehörden informieren.
Bei Ankündigungen weniger schwerer Taten (Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut) erlaubt §34 StGB die Durchbrechung der Schweigepflicht. Bei einem derartigen „rechtfertigenden Notstand" darf die Schweigepflicht aber nur durchbrochen werden, wenn diese vier Bedingungen erfüllt sind:

- Die Gefahr muss konkret und gegenwärtig sein.
- Die Durchbrechung der Schweigepflicht muss geeignet und angemessen sein, um die Gefahr abzuwenden.
- Es steht kein milderes Mittel als die Verletzung der Schweigepflicht zur Verfügung, um die Gefahr abzuwenden.
- Eine Abwägung ergibt, dass das Schutzinteresse gegenüber der Schweigepflicht wesentlich überwiegt.

Kindeswohlgefährdung muss (§138 StGB) bzw. darf (§32 StGB) nur angezeigt werden, wenn sie unter einen der beiden Paragrafen fällt.
Keine Anzeige darf erstattet werden, wenn die Tat in der Vergangenheit lag und nicht mehr verhindert werden kann.

Es gibt immer wieder Vorstöße vom Gesetzgeber, zum Schutz der Allgemeinheit möglichst lange auf die Verbindungsdaten zugreifen zu können. So wurden erneut Gesetzesentwürfe zur Vorratsdatenspeicherung vorgelegt, die sich auf die Anonymität im Internet allgemein auswirken könnten.

7. Ausblick

Ab dem 25.Mai 2018 gilt in ganz Europa die Europäische Datenschutz-Grundverordnung (EU DS-GVO). Bis dahin muss sie in jedem europäischen Land in ein neues Datenschutzgesetz umgesetzt werden. Die EU DS-GVO enthält einige sogenannte Öffnungsklauseln, d.h. an diesen Stellen darf die nationale Gesetzgebung von der GVO abweichen. Wie diese gestaltet werden, ist noch offen. Deutschland hat im Februar 2017 zwar ein neues BDSG vorgelegt, aber daran kann sich noch einiges ändern.

Absehbar sind folgende Entwicklungen (siehe auch folgende Pressemitteilung):
Es wird strengere Vorgaben geben zu

- Dokumentation der Risikofolgenabschätzung
- Altersnachweis (ausgenommen Präventions- und Beratungsangebote)
- Nachweis einer Einwilligung
- Schweigepflicht bei ADV-Verträgen

Dass der Gesetzgeber auch an anderer Stelle nachbessern muss, um die Vertraulichkeit psychosozialer Onlineberatung zu schützen, zeigt eine Stellungnahme der DGOB und des DGSF: *„Die Vertraulichkeit bei psychosozialer Onlineberatung sollte gesetzlich genauso geschützt werden wie eine anonyme Telefonberatung. Das ist in Deutschland aufgrund der aktuellen Gesetzesbestimmungen – Vorratsdatenspeicherung, Telekommunikationsgesetz, „BKA-Gesetz", Strafgesetzbuch – nicht der Fall: bieten psychosoziale Berufsgruppen anonyme Onlineberatung an, sind sie nicht ausreichend als „Berufsgeheimnisträger" geschützt."* Die gesamte Stellungnahme kann hier nachgelesen werden: https://idw-online.de/de/news678373.

8. Auf der sicheren Seite

Im Ergebnis passen die technischen und organisatorischen Maßnahmen für den Datenschutz an allen entscheidenden Stellen im Arbeitsalltag der bke-Onlineberatung zum fachlichen Anspruch auf Vertraulichkeit der bke. So bilden das Selbstverständnis und das Profil der bke, die gesetzlichen Anforderungen an den Datenschutz und die Qualitätsentwicklung der bke-Onlineberatung gemeinsam ein Paar.

Niemand muss Angst haben, einen Vertrauensbruch zu begehen, und Ratsuchende können sicher sein, dass nichts „hinter ihrem Rücken" stattfindet. Dank verständlicher Regeln für Betreiber, Beraterteam und Ratsuchende ist für alle Beteiligten klar, auf was sie sich einlassen und was sie dafür tun müssen. Diese Regeln werden in einem Datenschutz-Leitfaden festgehalten, der Bestandteil des Kooperationsvertrages zwischen den teilnehmenden Erziehungsberatungsstellen und der bke ist. Die Ratsuchenden finden alle relevanten Informationen zum Umgang mit ihren Daten in der verständlich verfassten Datenschutzerklärung und den umfassenden Nutzungsbedingungen der bke-Onlineberatung.

So stimmen der „gefühlte" und der reale Datenschutz überein. Und wenn es hin und wieder zu Verunsicherungen bei den Mitarbeitenden, der Geschäftsführung oder dem Vorstand einzelner Erziehungsberatungsstellen und Fragen wie "Dürfen wir das so machen?" kommt, so ist das ein gutes Zeichen für die Sensibilisierung, die stattgefunden hat.

Zudem ist allen Beteiligten klar, dass eine Datenschutz-Organisation einer ständigen Weiterentwicklung unterliegt, die fester Bestandteil der Qualitätsentwicklung der bke ist. Man kann also sagen, der bke ist es gelungen, einen "gelebten" Datenschutz zu organisieren.

Weitere Informationsquellen

Bundesdatenschutzgesetz (BDSG)
https://www.gesetze-im-internet.de/bdsg_1990/BDSG.pdf

Europäische Datenschutz-Grundverordnung
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)
https://www.bfdi.bund.de/DE/Home/home_node.html

Gesellschaft für Datenschutz und Datensicherheit
https://www.gdd.de/

http://www.vertraulichkeit-datenschutz-beratung.de/index.htm