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

8. Jahrgang, Heft 2, Artikel 6
Oktober 2012

Der Datenschutzassistent als Hilfsmittel beim Erstellen eines öffentlichen Verfahrensverzeichnisses [1]

Andreas Wimmer

Zusammenfassung
Datenschutz und Datensicherheit sind Grundlage für eine vertrauensvolle Beziehung zwischen BeraterIn und KlientIn. Gesetzliche Rahmenbedingungen fordern die Betreiber einer Onlineberatungsplattform auf, den Umgang mit den Daten der KlientInnen transparent offenzulegen. Das öffentliche Verfahrensverzeichnis soll hierfür die Grundlage sein. Die Erstellung kann durch den Einsatz eines Onlineassistenten, erreichbar unter http://www.mein-datenschutzassistent.de, erheblich erleichtert werden.

Schlüsselwörter
Datenschutz, Informationssicherheit, BDSG, Klientenschutz, Online-Beratungsplattform beranet, mein-datenschutzassistent.de, Datensicherheit, Transparenz, Verschlüsselung

Abstract
Privacy and data security are the basis for a trusting relationship between counsellor and client. Legal framework (in Germany) asks the operator of an online consultation platform to disclose the use of the data of the clients transparently. The "öffentliches Verfahrensverzeichnis" (public process directory) should be the basis for this transparency. The preparation of this "Verfahrensverzeichnis" can be greatly facilitated by the use of an online tool like http://www.mein-datenschutzassistent.de.

Keywords
Privacy, data security, client protection, transparency, online consultation platform beranet, encoding

Autor
- **Andreas Wimmer**
- Geschäftsführer der Internetagentur zone35
- Verantwortlich für die strategische Entwicklung der Online-Beratung bei beranet.de
- Plant seit 15 Jahren technische Lösungen von Mensch zu Mensch
- **Kontakt:** zone35 GmbH & Co. KG
  Wilhelmstr. 118
  10963 Berlin
  Web: http://www.beranet.de
  E-Mail: a.wimmer@zone35.de

1. Einleitung

Psychosoziale Beratung ist nur im vertraulichen und geschützten Rahmen sinnvoll. Mit dem Einzug der computervermittelten Kommunikation erfüllt die eingesetzte Technik die Funktion des Kommunikationskanals. Im Vergleich zu den bis dahin verwendeten Kommunikationsarten, wie dem persönlich geführten Gespräch oder Telefonat, hinterlässt dieser, noch relativ junge, Kanal bei der Übermittlung der Informationen Datenspuren - und zwar nicht nur im Internet.

Sowohl auf dem PC des Empfängers und Senders, als auch auf dem Internetserver, über den die Daten transferiert und gespeichert werden, werden personenbezogene Informationen abgelegt.

Das Gefühl, in guten Händen zu sein, ist von der Qualität der Beratung, der Sicherheit der Lösung und dem verantwortungsvollen Umgang mit den persönlichen Daten abhängig. Diese drei Faktoren sind für Ratsuchende essentiell, um sich, genau wie in einem persönlichen Gespräch, öffnen zu können. Grundlage dafür ist das Vertrauen in die Beratung und die verwendete Software. Durch eine transparente Darstellung des Umgangs mit den persönlichen Daten kann Vertrauen weiter gefestigt und gleichzeitig den gesetzlichen Anforderungen genügt werden. Jedoch ist auch zu beachten, dass die Datenverarbeitung in der Regel auf Dienstleister übertragen wird. Im Rahmen der Online-Beratung ist der Hostingpartner der technische Ansprechpartner, der Ihre Software wartet. Auch hier muss Transparenz gewahrt werden. Der Gesetzgeber fordert einen verantwortungsvollen Umgang mit persönlichen Daten und schreibt dies auch vor.

Neben der eigentlichen Begriffsklärung ist ebenso von Relevanz, wer mit welchen Daten wie umgeht und wie der transparente Umgang mit den Daten dokumentiert werden kann. Hierzu wurde in 2010 das Projekt http://www.mein-Datenschutzassistent.de in Kooperation mit dem Paritätischen Gesamtverband und unserem Datenschutzbeauftragten Markus Pleyer, tätig beim Paritätischen Wohlfahrtsverband, Landesverband Berlin e.V., umgesetzt. Auch als Betreiber der bundesweit meist genutzten Online-Beratungslösung stellte sich für uns immer wieder die Frage, wie den Datenschutzanforderungen genügt werden kann, denen jeder Betreiber einer Online-Beratungsstelle unterworfen ist. Die Entwicklung der Software http://www.mein-Datenschutzassistent.de soll zum einen bei der Konzeption der virtuellen Beratungsstelle unterstützen und auf die zu klärenden Punkte hinweisen und zum anderen die Erstellung des öffentlichen Verfahrensverzeichnisses vereinfachen.

2. Externe Dienstleister und Daten

Grundsätzlich zu klären ist, wer Zugriff auf die Daten erhält und welche gesetzlichen Verpflichtungen sich hieraus ergeben. Der Gesetzgeber definiert, dass nach §11 Absatz 5 des BDSG auch bei Wartung und Pflege von Software, sofern die Zugriffsmöglichkeit nicht ausgeschlossen werden kann, bereits Auftragsdatenverarbeitung vorliegt. Somit ist eine Vereinbarung zwischen dem Auftraggeber, dem Betreiber der virtuellen Beratungsstelle und dem technischen Dienstleister zu erstellen. Die Auftragserteilung hat schriftlich zu erfolgen und die in §11, Absatz 2 benannten Punkte zu enthalten, wie zum Beispiel: Gegenstand und Dauer, Löschung und Sperrung von Daten, Kontrollrechte, Weisungsbefugnisse und natürlich Rückgabe nach Beendigung des Vertragsverhältnisses. Somit ist bei dem Betrieb einer virtuellen Beratungsstelle darauf zu achten, dass diese Vereinbarung vorliegt.

3. Informationssicherheit

Die Sicherheit der Daten, auch Informationssicherheit genannt, ist essentiell. Es wird hierbei zwischen der Vertraulichkeit, der Verfügbarkeit und der Authentizität der hinterlegten Daten unterschieden. Gefordert ist besonders die Vertraulichkeit der Daten, was bedeutet, dass sichergestellt werden muss, dass nur ein beschränkter, genau definierter Empfängerkreis Zugriff auf die Inhalte erhält. In der Regel sind das Ratsuchender und Berater, in anderen Beratungssettings sind auch größere Personenkreise denkbar. Aber auch die Verfügbarkeit der Informationen ist von hoher Relevanz für die Informationssicherheit der Daten. Das wird üblicherweise über technische Systeme sichergestellt. Letztendlich ist jedoch auch die Datenintegrität von großer Bedeutung für die Beratung, was bedeutet, dass die Daten den korrekten Inhalt darstellen und nicht modifiziert werden.

4. Datenschutz ist ein Grundrecht

Somit hat die Informationssicherheit nicht das Ziel, grundsätzlich die Sicherheit von Daten zu gewährleisten, sondern stellt die Person und deren persönliche Daten in den Vordergrund. Es soll sichergestellt werden, dass kein Missbrauch erfolgt und die informationelle Selbstbestimmung gewährleistet wird. Diese beschreibt die Freizügigkeit eines jeden, über die Preisgabe und Verwendung seiner personenbezogenen Daten selbst bestimmen zu können. Art. 2, Abs. 1 des Grundgesetzes, beschreibt hierbei das allgemeine Persönlichkeitsrecht. Leider hatte eine Erweiterung des Grundrechtes Datenschutz bisher noch keine Mehrheit im Deutschen Bundestag erhalten, jedoch formuliert auch Art. 8 der EU Grundrechtecharta das Recht auf Entscheidungsfreiheit für eigene personenbezogene Daten.

5. Vertrauen ist gefragt

Allein der Umstand, dass es die digitale Datenverarbeitung möglich macht, unbegrenzte Kopien anzufertigen und Daten zu manipulieren und dies nur mit erheblichem Aufwand nachgeprüft werden kann, ist ein hoher Verunsicherungsfaktor für die Anwender von digitalen Systemen. Somit ist davon auszugehen, dass schon der Umstand, dass der einzelne Bürger nicht weiß, wie mit seinen Daten umgegangen wird, ein Auslöser sein kann, um Verhaltensänderungen im Umgang mit den persönlichen Daten stattfinden zu lassen. Jeder ist sich heutzutage bewusst, dass die Authentizität von Webseiteninhalten nur durch die Gesamtbetrachtung eines Internetauftrittes erfolgen kann: Ob dies nun das Google Ranking ist, die Querverweise von anderen seriösen Webseiten, ein korrektes Impressum, ein Gütesiegel wie das des Unabhängigen Landeszentrum für Schleswig Holstein oder auch das von der HON Stiftung entwickelte Zertifikat hängt von unterschiedlichen Faktoren ab. Für den Besucher einer Webseite ist es wichtig, nicht nur die Glaubwürdigkeit einschätzen zu können, sondern auch zu erkennen, wie mit den hinterlegten Daten umgegangen wird. Somit ist auch hierbei Medienkompetenz erforderlich, um eine glaubwürdige Einschätzung treffen zu können.

Gerade die Online-Beratung setzt auf das Vertrauensverhältnis zwischen BeraterIn und Ratsuchendem und selbstverständlich auch auf die Datensicherheit der dazwischen geschalteten technischen Systeme. Daher gilt es, die Kommunikationsplattform, über welche dieser Datenaustausch stattfindet, nicht nur technisch sicher, sondern auch transparent und authentisch zu gestalten, um die erforderliche Vertrauensbasis entwickeln zu können. Dies erfordert auch, dass in der Online-Beratung offenzulegen ist, welche Daten erfasst, welche wie lange gespeichert, für was verwendet und wann gelöscht werden.

6. Das Bundesdatenschutzgesetz

Der Umgang mit sensiblen Daten wird vom Gesetzgeber streng geregelt. Die gesetzlichen Vorgaben sind hierbei eindeutig (§4 BDSG) und verpflichten den Betreiber einer Webseite oder Online-Beratungsstelle dazu, den Umgang mit personenbezogenen Daten offenzulegen. Dabei muss Auskunft über sämtliche erhobene personenbezogene Daten, den Zweck der Datenerhebung, den Zugriff auf die Daten und die Löschfristen der Daten gegeben werden.

6.1 Was ist erlaubt, was nicht? Eine kleine Anleitung

Nicht nur Online-Beraterinnen und -Berater stehen oftmals vor der Frage, was ihnen rechtlich erlaubt und was verboten ist. Zur Einstimmung auf das Thema finden Sie hier einige generelle Leitsätze, die aus den Vorgaben des Bundesdatenschutzgesetzes (BDSG) abgeleitet sind.

Das dürfen Sie in keinem Fall:

- Personendaten ohne eine Erlaubnis durch Gesetze oder den Betroffenen selbst verarbeiten.
- Sich vom Betroffenen generell einwilligen lassen, dass dessen Daten verwendet werden.
- Den Betroffenen im Unklaren lassen, welche Daten über ihn verwendet werden.
- Ohne Kontrolle sein, wer, welche Personendaten zu welchem Zweck verwendet; etwa wenn BeraterInnen ihre Passwörter weitergeben oder Personendaten ungesichert per E-Mail versandt werden.
- Personendaten im PC ausschließlich lokal abspeichern, ohne Sicherung gegen Verlust oder Veränderung.
- Namentlich über Betroffene mit Kollegen reden, die nichts mit dem Beratungsfall zu tun haben.
- Nachfragenden Behörden oder Angehörigen bereitwillig Auskunft über KlientInnen geben, ohne dass diese davon wissen oder dem zugestimmt haben.

Das dürfen Sie:

- Verwendung von Personaldaten zu Verwaltungszwecken und aus technischen Gründen, sofern das dem Betroffenen bekannt ist.

- Aufbewahren von Personendaten über einen langen Zeitraum, sofern es dafür einen Grund gibt und dieser dem Betroffenen bekannt ist, etwa als Nachweis zur Verwendung von öffentlichen Geldern.
- Im Kollegenkreis anonym über Betroffene reden.
- Personendaten ungefragt weitergeben, wenn es ein Notfall oder die Abwendung von Gefahren erforderlich macht, um zu helfen.
- Personendaten ungefragt weitergeben, wenn damit eine schwere Straftat verhindert werden kann.

7. Das öffentliche Verfahrensverzeichnis

Staatliche oder auch private Stellen, die personenbezogene Daten erfassen und verarbeiten, müssen jederzeit darüber Auskunft geben können, welche Daten erfasst werden, zu welchem Zweck die Datenerhebung erfolgt, was mit den Daten geschieht und wann die Daten gelöscht werden. Die geforderten Inhalte des öffentlichen Verfahrensverzeichnisses sind ebenfalls in §4 BDSG festgeschrieben.

Diese Auskunft, die jeder Person zugänglich sein muss, von der personenbezogene Daten erhoben, gespeichert und verarbeitet werden, nennt man öffentliches Verfahrensverzeichnis.

7.1 Wohin mit dem öffentlichen Verfahrensverzeichnis?

Die Ausweisung des öffentlichen Verfahrensverzeichnisses sollte an einer gut aufzufindenden Stelle erfolgen, möglicherweise im Impressum. Dieses muss ohnehin von jeder Seite eines Webangebotes aus erreichbar sein, daher erscheint die Einbindung des ÖVV an dieser Stelle sinnvoll. Letztlich bleibt es jeder Einrichtung selbst überlassen, ob und wo sie das ÖVV ausweist. Auf Anfrage von Personen, deren personenbezogene Daten gespeichert werden, muss das ÖVV in jedem Fall herausgegeben werden können.

7.2 Was leistet der Assistent?

Der Datenschutz-Assistent kann helfen, ein öffentliches Verfahrensverzeichnis zu erstellen. Sowohl Beratungsstellen, die die Beratungslösung beranet einsetzen, als auch alle anderen Einrichtungen, die personenbezogene Daten erheben, finden im Assistenten ein komfortables Werkzeug, um schnell und einfach ein passendes öffentliches Verfahrensverzeichnis zu erstellen.

7.3 Wo sind die Grenzen des Assistenten?

Aufgrund der Vielzahl der möglichen Rechtsformen, Datentypen, Verarbeitungszwecke und rechtlichen Hintergründe können wir keine hundertprozentige Rechtssicherheit garantieren. Wir erheben keinen Anspruch auf hundertprozentige rechtssichere Vollständigkeit des ÖVV. In jedem Fall empfehlen wir eine nachfolgende Prüfung des erstellten öffentlichen Verfahrensverzeichnisses durch einen Rechtsanwalt und übernehmen keine Haftung für rechtliche Probleme, die eventuell aus der Verwendung eines hier erstellen öffentlichen Verfahrensverzeichnisses erwachsen.

Vor der Erstellung eines öffentlichen Verfahrensverzeichnisses, sollten folgende Daten zusammentragen werden:

- Kontaktdaten und Verantwortliche Ihrer Einrichtung
- Eine Liste ALLER erfassten Datentypen, ALLER Verwendungszwecke und ALLER Löschfristen
- Technische Daten zu Ihrer Webseite/Beratungsstelle (verwendete technische Lösung für Webseite oder Beratungsstelle, Informationen über Erfassung von Cookies, Speicherung von Verbindungsdaten)
- Informationen über das generelle Vorgehen Ihrer Einrichtung/Firma im Hinblick auf Datensicherheit (technische und administrative Vorkehrungen).

Der Datenschutzassistent wurde mit größtmöglicher Sorgfalt erstellt und nach den Vorgaben des Bundesdatenschutzgesetzes angelegt. Letztlich hängt es aber auch von den ausfüllenden Personen ab, ob das generierte öffentliche Verfahrensverzeichnis vollständig ist.

Anmerkungen:

[1] Der Artikel bezieht sich auf die deutsche Rechtslage.