Datenschutz bei der Arbeit mit besonders schutzbedürftigen Geflüchteten

Handreichung für die Beratung

Inhaltsverzeichnis

Ziel dieser Handreichung

Der Einhaltung von Datenschutzregeln kommt beim Umgang mit Geflüchteten eine besondere Bedeutung zu. Menschen, die vor Verfolgung fliehen, brauchen die unbedingte Sicherheit, dass bei der Aufnahme und Beratung die persönlichkeitsschützenden Regeln des Rechtsstaates eingehalten werden. Gerade gegenüber Menschen, die nach Deutschland geflohen sind, muss der Datenschutz als menschenrechtsschützende Norm sicher eingehalten werden.

Gleichzeitig besteht beim Umgang mit personenbezogenen Daten von Geflüchteten oft große Verunsicherung beim Hilfenetzwerk.

? Was darf und soll wie und für wen dokumentiert werden?

? Wie kann sichergestellt werden, dass die betroffenen Geflüchteten umfassend über den Umfang der Datenerhebung und die Verwendung informiert sind, dass sie damit einverstanden sind und dass ihnen dadurch kein Schaden entsteht?

Diese Handreichung richtet sich daher an zwei Adressat*innengruppen.

Einerseits soll sie den im gesetzlichen Sinne „Verantwortlichen“, also den datenverarbeitenden Organisationen oder Unternehmungen Hinweise auf die Anforderungen einer datenschutzkonformen, betrieblichen Organisation geben. Denn die Festlegung betrieblicher Abläufe und Vorgaben durch Richtlinien, Arbeitsanweisungen etc. ist Aufgabe der Führungsebene einer, im Sinne der Datenschutzgesetzgebung, verantwortlichen Stelle. Datenschutzrechtliche Bewertungen zu Verfahrensweisen, Abwägungen und Rechtsgrundlagen können und dürfen nicht auf einzelne Beschäftigte abgewälzt werden. Eine verantwortliche Ansprechperson muss klar benannt werden.

Andererseits soll die Handreichung den in der Arbeit mit Geflüchteten Tätigen, unabhängig von den beschriebenen nötigen Vorgaben, die Grundzüge datenschutzrechtlicher Anforderungen erläutern und anhand praktischer Beispiele illustrieren und ihnen mehr Handlungssicherheit vermitteln.

Ohne Rechtsgrundlage keine Verarbeitung („Verbot mit Erlaubnisvorbehalt“)

Jede beabsichtigte Verarbeitung personenbezogener Daten, vom Sammeln (Erheben, Aufschreiben, ...) über jegliche denkbare Verwendung bis hin zum Löschen, muss entweder durch ein Gesetz oder durch die betroffene Person selbst (durch Einwilligung) erlaubt sein. Um rechtmäßig Daten zu verarbeiten, ist es nötig, zuvor die Erlaubnisgrundlage geklärt zu haben.

Zweckbindung

Mit der Rechtsgrundlage eng verknüpft ist der zulässige Zweck, für den die personenbezogenen Daten erhoben und verwendet werden dürfen. Die Zulässigkeit einer Verarbeitung bestimmter Daten für einen bestimmten Zweck erlaubt nicht automatisch die Verarbeitung für andere Zwecke. So kann die Information über die Homosexualität einer geflüchteten Person für therapeutische Zwecke erforderlich sein und für diesen Zweck erfragt werden; anderen in einer Sammelunterkunft Untergebrachten darf sie jedoch, zur Vermeidung von Diskriminierung, nicht bekannt werden.

Erforderlichkeit

Jede beabsichtigte Erhebung oder sonstige Verarbeitung personenbezogener Daten muss nötig sein, um den jeweils rechtmäßigen Zweck zu erzielen. Zur Umsetzung der Erforderlichkeit dienen auch Datenminimierung und Datenvermeidung. So ist beispielsweise die Information über eine Gehbehinderung bei der Auswahl der Unterbringung relevant, nicht jedoch bei der Anmeldung zu einem Sprachkurs (es sei denn, der Kurs fände in für Gehbehinderte schwer zugänglichen Räumlichkeiten statt).

Die Erforderlichkeit endet in der Regel nach bestimmten Zeiträumen.
Daher muss durch Fristen und Vorgaben sichergestellt werden, dass Daten gelöscht werden, sobald sie nicht mehr erforderlich sind.

Transparenz

Menschen sollen immer wissen können, wer welche ihrer Daten zu welchen Zwecken verarbeitet. Wer personenbezogene Daten verarbeitet, muss diese Informationen daher in für Betroffene verständlicher Form vermitteln.

Richtigkeit

Wenn personenbezogene Daten verarbeitet werden, müssen sie korrekt abgelegt und wiedergegeben werden. Dies ist in der Arbeit mit Geflüchteten besonders wichtig, weil falsche Angaben, z.B. über den Fluchtweg oder die ethnische Zugehörigkeit, zu Nachteilen für die Geflüchteten, z.B. zur Ablehnung des Asylantrags oder zur Abschiebung, führen können.

Angemessene Schutzmaßnahmen

Jegliche Verarbeitung personenbezogener Daten muss so erfolgen, dass wirksame Schutzmaßnahmen eine Begrenzung auf das Erlaubte sicherstellen.
Dies betrifft beispielsweise Zugriffsbegrenzungen bei den verwendeten Informationstechnik (IT) Systemen, die Verwendung von Verschlüsselung oder die Definition klarer Abläufe und Zuständigkeiten. So sollen beispielsweise ausländische Geheimdienste die E-Mail-Kommunikation nicht mitlesen können.

Was ist Datenschutz?

Datenschutz ist Menschenrecht und Persönlichkeitsschutz, der allen Menschen zusteht.

Schutzsuchende haben daher ein Grundrecht auf Datenschutz, welches das Bundesverfassungsgericht auch „Recht auf informationelle Selbstbestimmung“ nennt.
Nachlesen kann man dies in der Europäischen Grundrechte-Charta (Art. 8 GRCh) und im Grundgesetz (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG). Es beinhaltet den Anspruch von Menschen, dass die Verarbeitung ihrer personenbezogenen Daten klaren Regeln und Prinzipien folgt. Diese sind grundlegend in der europäischen Datenschutzgrundverordnung (DSGVO) und auch in Einzelgesetzen geregelt, wie z.B. im Asylgesetz im Aufenthaltsgesetz oder in EU-Verordnungen.

Verantwortlichkeit und besonderer Schutzbedarf

Die Einhaltung und Umsetzung dieser gesetzlichen Vorgaben ist Aufgabe der sogenannten datenschutzrechtlich „Verantwortlichen“. Dies sind die Stellen, die Daten der betroffenen Personen verarbeiten bzw. durch ihre Beschäftigten verarbeiten lassen – zum Beispiel eine Behörde, ein Unternehmen, eine Beratungs- oder Betreuungseinrichtung. Aber auch eine unabhängig tätige Beraterin ist Verantwortliche. Die Verantwortlichkeit liegt immer bei der Leitung der jeweiligen Stelle, die daher ihren Beschäftigten klare, rechtssichere Vorgaben für die Verarbeitung personenbezogener Daten machen muss. Dies entbindet die Beschäftigten allerdings nicht davon – gemäß den Vorgaben des Arbeitgebers – mit den Daten korrekt umzugehen.
Missachten Beschäftigte bewusst die Gesetze oder die betrieblichen Vorgaben, so können sie hierfür selbst haftbar gemacht werden.

Sowohl für die Leitung der verantwortlichen Stelle als auch für die Betreuer*innen und Berater*innen Geflüchteter besteht daher die Verpflichtung, den Datenschutz einzuhalten, die Persönlichkeitsrechte der Betroffenen zu wahren und dazu beizutragen, dass diese selbst ihre Datenschutzrechte wahrnehmen können.

Bei Geflüchteten bestehen in Bezug auf ihre Daten regelmäßig hohe Anforderungen an den Datenschutz. Geflüchtete Menschen befinden sich in einer schwierigen, oft als bedrohlich empfundenen Lebenssituation, z.B. nach traumatischen Erlebnissen, wegen Krieg und Vertreibung, (drohender) Verfolgung, auf Grund beschränkter materieller Ressourcen oder wegen Gesundheitsbeeinträchtigungen.

Werden Geflüchtete durch Personen unterstützt, die einer beruflichen Schweigepflicht unterliegen (Ärzt*innen, Psycholog*innen und Therapeut*innen, Rechtsanwält*innen, staatlich anerkannte Sozialarbeiter*innen), so unterliegen die anvertrauten Informationen einer erhöhten Vertraulichkeit und Geheimhaltung. Dies wird über den Datenschutz hinaus durch § 203 des Strafgesetzbuchs sichergestellt, so dass Geflüchtete sich umfassend offenbaren können, ohne dadurch Nachteile befürchten zu müssen. Da viele besondere Schutzbedarfe geflüchteter Menschen äußerlich nicht sichtbar sind, sondern ihre Versorgung davon abhängt, ob eine Person sich anvertraut, ist eine aktive Kommunikation und Information geflüchteter Menschen über Datenschutz und Schweigepflicht besonders wichtig. Gerade bei angst- und schambesetzten Themen können diese Informationen die nötige Sicherheit geben, sich zu öffnen.

Hinweise für die Anwendung in der Beratung

1. Leitung und Arbeitgeber*innen

Die Einhaltung der oben dargestellten Prinzipien und die Ansprüche der Betroffenen auf Datenschutz müssen durch die verantwortliche Stelle sichergestellt werden. Dazu gehören auch Richtlinien und Arbeitsanweisungen, die den Umgang mit der IT allgemein und den Umgang mit personenbezogenen Daten und Dokumenten im Besonderen vorgeben.

Bei der Suche nach der Rechtsgrundlage bei der Verarbeitung von Daten Geflüchteter kommen Gesetze (z.B. Aufenthaltsgesetz, Sozialgesetzbuch), Verträge (z.B. Behandlungs-, Beratungs-, Anwalts- oder Mietvertrag) oder Einwilligungen betroffener Geflüchteter (z.B. in Fällen einer geplanten Datenweitergabe an sonstige, nicht grundsätzlich berechtigte Dritte) in Betracht (Art. 6 Abs. 1 DSGVO). Verantwortliche Stellen können sich in bestimmten Fällen auch auf „berechtigte Interessen“ berufen, wenn nicht die schutzwürdigen Interessen der geflüchteten Personen überwiegen. Hierbei ist allerdings zu beachten, dass eine ernsthafte Abwägung erfolgen und auch dokumentiert werden muss.

Verarbeitungen, die sich auf eine Einwilligung Betroffener stützen sollen, müssen zuvor so erklärt werden, dass (ebenso wie bei einer Schweigepflichtentbindung) eindeutig verständlich ist, welche Daten für welchen Zweck durch wen verarbeitet und evtl. weitergeben werden.
Die Erklärung muss freiwillig erfolgen und kann jederzeit widerrufen werden. Für diese Fälle muss eine sichere Umsetzung des Widerrufs garantiert sein, weswegen sich die Einwilligung als Rechtsgrundlage niemals für Fälle eignet, bei denen eine Rücknahme (z.B. technisch oder organisatorisch) gar nicht möglich wäre. Die erbrachte Einwilligung/Erklärung und der Widerruf sind angemessen zu dokumentieren. Erfüllt eine Einwilligung eine oder mehrere der Vorgaben (also die Freiwilligkeit, die klaren Informationen oder die Widerrufbarkeit) nicht, ist sie unwirksam und nicht als Rechtsgrundlage geeignet.

Innerhalb eines Beratungsteams müssen für die Einholung von Einwilligungen klare Voraussetzungen und Abläufe definiert sein.

→ Hinweise für Einwilligungen finden sich unter

https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Datenschutz/Einwilligung.html

→ Hinweise zu Schweigepflichtentbindungserklärungen finden sich unter

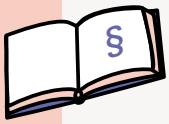
https://www.fruehehilfen.de/fileadmin/user_upload/fruehehilfen.de/pdf/Publikation-NZFH-Schweigepflichtentbindung-kommunizieren-Arbeitshilfe-Broschuere.pdf, sowie

https://www.datenschutzzentrum.de/artikel/202-1.html

Weit verbreitet, aber falsch ist es, sich eine Einwilligung der Betroffenen geben zu lassen, obwohl es eine rechtliche Grundlage für die Datenverarbeitung gibt (z.B. Gesetz, Vertrag).
Dadurch erhält der Betroffene den falschen Eindruck, frei entscheiden und diese Entscheidung zurücknehmen zu können.

Die verantwortliche Stelle muss auch (durch verbindliche Definition klarer Abläufe) sicherstellen, dass jegliche Datenverarbeitung für die betroffene geflüchtete Person erkennbar und verständlich (transparent) ist. Dies gilt nicht nur bei der Einholung von Einwilligungen, sondern für jede Verarbeitung. So ist bei der ersten Datenerhebung (z.B. beim Anlegen einer Beratungsakte) mitzuteilen, welche Daten für welche Zwecke auf Grund welcher Rechtsgrundlage verarbeitet und evtl. auch weitergegeben werden, sowie welche Rechte (z.B. Auskunft, Berichtigung, Löschung) Betroffene haben.

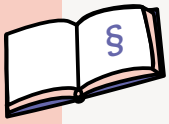
Eine mehrsprachige Vorlage für so eine datenschutzrechtliche Aufklärung findet sich z.B. in der Toolbox für besondere Schutzbedarfe der BAfF e.V. (Art. 12-14 DSGVO).



Macht eine geflüchtete Person von ihrem Auskunftsrecht Gebrauch, auf das jeder Mensch Anspruch hat (Art. 15 DSGVO), so muss die verantwortliche Stelle in der Lage sein, diese Auskunft unverzüglich zu erteilen. Auch hier ist es also nötig, rechtzeitig entsprechende verbindliche Abläufe zu definieren. Dieser Anspruch ist umfassend und bezieht sich auf alle zur anfragenden Person vorhandenen Daten.
Sie umfasst daher auch interne Aufzeichnungen wie beispielsweise Gesprächsprotokolle.
Da eine Auskunftsverweigerung nur in wenigen – speziell zu begründenden – Fällen (z.B. wegen einer Sicherheitsgefährdung) gerechtfertigt ist, kommt der Datenminimierung schon bei der Erhebung eine ganz besondere Rolle zu.

Als Faustregel lässt sich festhalten, dass man keine Daten erfassen sollte, von denen man später nicht wollen kann, dass sie der betroffenen Person bei einer Auskunftserteilung bekannt werden, beispielsweise wertende Beschreibungen über die Person, die nicht nötig sind.

Weitere Datenschutzansprüche der Betroffenen sind u.a.:



- Recht auf Berichtigung, wenn unzutreffende Daten gespeichert sind (Art. 16 DSGVO)
- Recht auf Datenlöschung , wenn die Speicherung nicht mehr nötig oder diese unzulässig ist (Art. 17 DSGVO)
- Recht auf Beschwerde bei der zuständigen Datenschutzbehörde (Art. 77 DSGVO)
- Recht auf Schadenersatz bei einem durch eine unzulässige Datenverarbeitung verursachten materiellen oder immateriellen Schaden – dies gilt z.B. für den Kontrollverlust über die eigenen Daten bei einer unzulässigen Datenweitergabe (Art. 82 DSGVO). Beispielsweise wurde einer betroffenen Person wegen unzulässiger Weitergabe von Vertragsdaten an die SCHUFA ein Betrag von 5.000 Euro zugesprochen.

Die verantwortliche Stelle ist auch für die Ergreifung der angemessenen Schutzmaßnahmen zur Sicherstellung von Integrität und Vertraulichkeit der Daten und ihrer Verarbeitung zuständig, also für den korrekten Einsatz der Informationstechnik und den sicheren Umgang mit Akten.
Die Verantwortlichkeit erstreckt sich auf alle Organisationsaspekte der Datenverarbeitung, also die Beschäftigung der jeweils eingebundenen Personen, die Einbeziehung von IT-Dienstleister*innen sowie von anderen Auftragnehmer*innen bis hin zu Dolmetschenden/Sprachmittler*innen.

Insbesondere zum sicheren Einsatz von IT müssen folgende Sicherheitsvorkehrungen getroffen werden:

- ☐ Zugang zum System nur nach sicherer, personengebundener Authentifizierung (Login). Bei einem System, das von mehreren Personen genutzt wird, muss sich jede Person separat authentifizieren.
- ☐ Orientierung der Rechte am „Need-to-know"-Prinzip, also an den zu erledigenden Aufgaben; die Rechte sollten also differenziert vergeben werden können.
- ☐ Durchführung und Kontrolle einer Nutzungsprotokollierung, um im Nachhinein feststellen zu können, wer konkrete Aktionen durchgeführt hat.
- ☐ Bei der kurzfristigen Nichtnutzung des Systems (nach z.B. 5 Minuten) wird zwangsweise ein Bildschirmschoner aktiviert.
- ☐ Regelmäßig – mindestens wöchentlich, besser täglich – ist auf einem gesonderten Datenträger eine Datensicherung vorzunehmen und in vor unberechtigtem Zugriff geschützter Umgebung aufzubewahren.

Es ist außerdem ein Verarbeitungsverzeichnis gemäß den Vorgaben des Art. 30 DSGVO zu führen, in dem die wesentlichen Angaben zu Prozessen („Verfahren") zu erfassen sind, in denen personenbezogene Daten verarbeitet werden.

Nähere Angaben hierzu finden sich unter

https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Allgemein/Verzeichnis-Verarbeitungstaetigkeiten.html

Haben in einer verantwortlichen Stelle mehr als 20 Personen Zugriff auf personenbezogene Daten, muss ein eigener Datenschutzbeauftragter bestellt werden.
An diese Person können sich alle Beteiligten in Zweifelsfragen zum Datenschutz wenden (Art. 37 ff. DSGVO, §§ 5 bzw. § 38 BDSG).

2. Beschäftigte und individuelle Beratende

Viele Beratende sind Quereinsteiger*innen bzw. haben kein umfangreiches Vorwissen zum Thema Datenschutz. Dies entbindet sie aber weder von der Einhaltung allgemeiner Datenschutzprinzipien noch von der Einhaltung datenschutzrechtlicher Vorgaben der Organisation, unter deren Dach oder in deren Auftrag sie tätig sind. Die Initiierung geeigneter Aus- und Fortbildung ist daher sowohl Aufgabe einer evtl. verantwortlichen Stelle als auch, im Falle individuell Beratender, deren eigene Aufgabe. Die über den Datenschutz aufklärende Person sollte ausreichende eigene Kenntnisse haben, nur so sind auch Rückfragen der Betroffenen möglichst sicher zu beantworten. Daher sollte, wenn intern keine ausreichenden Kenntnisse vorhanden sind, auch auf externe Schulungsangebote zurückgegriffen werden.

Unabhängig von der Einbindung in ein organisatorisches Regelwerk durch die verantwortliche Stelle lassen sich aus den oben dargestellten Datenschutzprinzipien grundlegende Anforderungen an datenschutzgerechte Verhaltensweisen in der Beratungsarbeit formulieren.

2.1 Beratungs- und Betreuungsgespräche

Bei Betreuungs- und Beratungsgesprächen muss sichergestellt werden, dass keine unbeteiligten und nichtberechtigten Personen mithören können. Dies erfordert in den meisten Fällen einen während des Gesprächs nur von den Gesprächsteilnehmern genutzten, abgeschlossenen Raum. Wenn Klient*innen zu einem Beratungsangebot begleitet werden, sollte nicht automatisch angenommen werden, dass die Begleitperson auch am Gespräch teilnimmt.
Nur auf ausdrücklichen Wunsch der begleiteten Person kann eine Teilnahme stattfinden.

Bedarf es einer Sprachmittlung, so ist darauf zu achten, dass diese vertrauenswürdig ist und ihrerseits die Vertraulichkeit der besprochenen Inhalte garantiert – entweder durch Zertifizierung oder aber explizite schriftliche Zusicherung. Für die Fälle der Beratung mit besonderem Schutzbedarf sollten sprachmittelnde Personen nicht nur sprachlich qualifiziert sein, sondern sich auch durch weiterführendes Material oder entsprechende Fortbildung das spezifische Vokabular und die damit verbundene Sensibilität angeeignet haben.

Werden digitale (öffentlich zugängliche) Übersetzungswerkzeuge verwendet, so ist darauf zu achten, dass keine Namen, präzise Ortsangaben oder sonstige eindeutige Informationen einfließen, aus denen auf die Identität der Person geschlossen werden kann.

2.2 Dokumentation

Sowohl bei der Aktenführung (Papier) als auch der Datenpflege (IT) ist darauf zu achten, dass die Unterlagen (Gesprächsprotokolle, Gutachten, behördliche Schreiben, Stellungnahmen, Krankenunterlagen) in verschlossenen Schränken und Räumen aufbewahrt werden, wenn sie nicht unmittelbar bearbeitet werden.

Generell gilt zur Einhaltung der Erforderlichkeit: Zu dokumentieren ist nur das, was nötig ist. Es ist zudem darauf zu achten, dass Namen von Personen in Dokumenten nur dann genannt werden, wenn es unbedingt erforderlich ist. Betroffene können alternativ durch ihre Rolle (geflüchtete Person, Patient*in, Proband*in, Mutter ...) beschrieben werden, so dass eine pseudonyme Weiternutzung (z.B. im Rahmen einer Supervision) einfacher und weniger fehleranfällig möglich ist.

2.3 Kommunikation

Bei praktisch jeder Kommunikation findet auch ein Datenaustausch über die geflüchtete Person statt, also eine Datenerhebung und -übermittlung. Dafür ist jeweils eine Legitimation (Rechtsgrundlage, s.o.) nötig. Auch wenn eine Legitimation besteht, sollten die Beteiligten ihren Austausch auf das beschränken, was unbedingt nötig ist (Erforderlichkeit).

Bei einem persönlichen Austausch (vor Ort oder per Telefon), sollte bei relevanten Vorgängen ein kurzer Vermerk erfolgen über Gesprächspartner*innen, Zeit, evtl. Ort, Thema und Inhalt sowie getroffene Absprachen zum weiteren Vorgehen. Bevor es zu einem Austausch über die geflüchtete Person kommt, muss sichergestellt werden, wer der Kommunikationspartner ist, ob dieser berechtigt ist, die Informationen zu erhalten, und ob er oder sie keine unberechtigten Zuhörer*innen hat.

Bei der Verwendung digitaler Kommunikationswege (E-Mail, Messenger) ist besonders auf eine datensparsame Darstellung zu achten (bspw. Signal, Threema, gesicherte Chatprogramme). Zumindest sensible Inhalte (ärztliche Unterlagen, Verfahrensdokumente) dürfen nur verschlüsselt übermittelt werden (z.B. unter Nutzung von PGP oder durch Nutzung einer verschlüsselten Austauschplattform wie z.B. Nextcloud).
Der Austausch verwendeter Schlüssel zwischen den Partner*innen darf nur über einen von der Informationsübertragung verschiedenen Weg erfolgen (z.B. Schlüssel via SMS und Datenaustausch per E-Mail).

Hinweise finden sich auch unter:

https://www.datenschutzzentrum.de/artikel/1177-Daten-verschluesselt-uebertragen-aber-wie.html

Bei Versendungen an eine Vielzahl von Personen (Mailverteiler) sind diese verdeckt zu adressieren (bei E-Mails durch bcc). Die Verwendung einer größeren Menge von Adressaten (die sich in diesem Zusammenhang nicht zu kennen brauchen) im offen sichtbaren Adressfeld ist unzulässig und kann Schadenersatzansprüche nach sich ziehen.

Bei Versendungen im Rahmen individueller, direkter Kommunikation ist hingegen darauf zu achten, dass aus Transparenzgründen alle Adressat*innen für alle Empfänger*innen erkennbar sind.

Auch bei der Kommunikation mit Geflüchteten selbst sollte man sich an die zuvor genannten Grundsätze halten, da Endgeräte und die Inhalte möglicherweise auch für Dritte einsehbar sind.

Die Weitergabe von Fotos oder Videos Geflüchteter sollte äußerst restriktiv behandelt werden. Eine Einwilligung der Betroffenen muss grundsätzlich vorher eingeholt werden.
Das Risiko, dass Personen auf Fotos durch Gesichtserkennungssoftware auch ohne Namensnennung identifiziert werden, ist hoch und kann für Geflüchtete lebensbedrohlich sein. Eine Veröffentlichung von Fotos sollte deshalb nur in Einzelfällen, nach Aufklärung über die Risiken und mit schriftlicher Einwilligung erfolgen.

Weiterführende Informationen und Unterstützung

- Detaillierte Informationen zum Datenschutz sowie Abdrucke der wesentlichen Rechtsgrundlagen finden sich in der Publikation Datenschutz in der sozialen Arbeit mit geflüchteten Menschen.
- Allgemeine Erläuterungen zu Datenschutzgrundlagen finden sich in der Handreichung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

  Bestehen für Beratende hinsichtlich des Datenschutzes in konkreten Anwendungsfällen Unsicherheiten, so können diese sich an die Datenschutzbeauftragten der Organisation wenden, in deren Auftrag sie tätig sind.

- Wenn keine Klärung herbeigeführt werden kann, so besteht auch die Möglichkeit, sich mit der Bitte um einen Rat an die zuständige Datenschutzbehörde zu wenden. Dies gilt natürlich in jedem Fall, wenn der Verdacht besteht, dass ein Datenschutzverstoß erfolgt ist.
  Erfolgt eine solche Beschwerde durch die betroffene Person, so muss die Datenschutzbehörde tätig werden.

  Die Adressen der zuständigen Behörden finden sich im Internet unter

  https://www.datenschutz.de/projektpartner/

Impressum

Herausgeberin:

ZIVILGESELLSCHAFTLICHE FACHSTELLE ZUR IDENTIFIZIERUNG UND UMSETZUNG BESONDERER schutz bedarfe

BAfF - Bundesweite Arbeitsgemeinschaft
der Psychosozialen Zentren für Flüchtlinge
und Folteropfer e. V.
Wilhelmstraße 115, 10963 Berlin, Germany

Web: www.baff-zentren.org

In Kooperation mit:

NETZWERK DATENSCHUTZEXPERTISE

Netzwerk Datenschutzexpertise
Kronprinzenstr. 76
53173 Bonn

Web: https://www.netzwerk-datenschutzexpertise.de/

Autor*innen: Thilo Weichert, Karin Schuler, Alva Träbert, Larissa Hilt

Gestaltung & Satz: Claire Schiffner

Die Publikation kann über den Online-Shop der BAfF bestellt werden:

http://www.baff-zentren.org/veroeffentlichungen-der-baff/shop/

Gefördert vom:

Gefördert vom Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend

im Rahmen des Bundesprogramms Demokratie leben!

Die Veröffentlichung stellt keine Meinungsäußerung des Bundesministeriums für Bildung, Familie, Senioren, Frauen und Jugend (BMBFSFJ) dar.