DATENSCHUTZHANDBUCH

Erklärungen und Verfahrensanweisungen für die Beratungsstellen des Netzwerks unabhängige Beratung

Netzwerk
unabhängige
Beratung

INHALT

I. VORWORT

Das vorliegende Muster des Datenschutzhandbuches soll den Beratungsstellen in der unabhängigen Teilhabeberatung als Anleitung für die Erstellung eines eigenen Datenschutzhandbuches sowie zur Etablierung und Sicherung des Datenschutzes in der Beratungsstelle dienen.

Das Datenschutzhandbuch und die darin enthaltenen Grundsätze über Erhebung, Umgang und Sicherung von personenbezogenen Daten der Ratsuchenden orientieren sich an dem Leitbild der Selbsthilfe und Selbstbestimmung in der Beratung. Dies bedeutet, dass die Beratenden nicht Sachwalter oder Vertreter der Ratsuchenden werden. Die Beratenden sollen begleiten und unterstützen. Ziel ist es, dass notwendige Anträge oder Anschreiben stets von den Ratsuchenden selbst verfasst werden. Die Beratenden übernehmen auch nicht ausschließlich die Kommunikation mit Dritten für die Ratsuchenden, sondern begleiten und unterstützen auch hier. Schlussendlich sollen die Beratenden stets gemeinsam mit den Ratsuchenden deren eigene Handlungen unterstützen und bei deren Realisierung helfen. Da die Beratenden in einem vertrauensvollen Verhältnis zu den Ratsuchenden stehen und diese begleiten, benötigen sie in ihrer eigenen Aktenverwaltung nur wenige Daten von den Ratsuchenden, da diese selbst handeln und kommunizieren. Persönliche Daten der Ratsuchenden, die von Dritten benötigt werden, können von den Ratsuchenden gegeben werden, so dass keine Notwendigkeit für die Beratenden in der Beratungsstelle besteht, diese zu erheben, zu speichern oder zu verarbeiten.

Das vorliegend abgebildete Datenschutzkonzept will durch Hinweise an die Ratsuchenden proaktiven Datenschutz erreichen. Es soll gewährleistet werden, dass die Daten durch die Beratungsstelle sicher verarbeitet werden. Darüber hinaus sollen die Ratsuchenden durch die Beratenden durch Fragen und Hinweise auf Aspekte des Datenschutzes hingewiesen und sensibilisiert werden.

Das Datenschutzhandbuch soll stetig fortgeschrieben werden.

II. ADRESSATEN DES DATENSCHUTZHANDBUCHES

Das Handbuch richtet sich an die Beratenden und die Ratsuchenden der Beratungsstelle.

Für die unabhängige Teilhabeberatung ist ein vertrauensvoller und korrekter Umgang mit den sensiblen personenbezogenen Daten der Ratsuchenden von größter Wichtigkeit. Ein solcher Umgang kann durch ein vertrauensvolles Zusammenwirken von Ratsuchenden und Beratenden erreicht werden.

Der Datenschutz bezweckt den Schutz des Rechts auf informationelle Selbstbestimmung, das aus dem allgemeinen Persönlichkeitsrecht in Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG hergeleitet wird.

III. DATENSCHUTZBEAUFTRAGTER

„Datenschutzbeauftragte(r) der Beratungsstelle … ist … Diese(r) ist wie folgt zu erreichen: (Kontaktdaten einsetzen).“

Aufgrund der Größe der Beratungsstelle sowie des Umfangs der Datenerhebung, Speicherung und Nutzung liegt eine verpflichtende Bestellung eines Datenschutzbeauftragten oder einer Datenschutzbeauftragten für die Beratungsstelle nicht vor. Nichtsdestotrotz sieht die Beratungsstelle es als eine Selbstverpflichtung an, einen Datenschutzbeauftragten oder eine Datenschutzbeauftragte zu benennen und diesen auch die nach dem Bundesdatenschutzgesetz festgelegten Befugnisse und Prüfungspflichten einzuräumen.

Ratsuchende können sich jeder Zeit vertrauensvoll an die Datenschutzbeauftragten wenden, die ihrerseits bezüglich dieser Anfrage einer Verschwiegenheitsverpflichtung unterliegen.

IV. GEWÄHRLEISTUNGSZIELE UND GRUNDSÄTZE FÜR DEN DATENSCHUTZ IN DER BERATUNGSSTELLE

Die Gewährleistungsziele des Datenschutzes in der Beratungsstelle entsprechen den Gewährleistungszielen des Standard-Datenschutzmodells der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder. Diese werden von der Beratungsstelle beachtet und umgesetzt.

Im Einzelnen:
- Datenminimierung
- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Nichtverkettung
- Transparenz
- Intervenierbarkeit

1. Datenminimierung

Das Gewährleistungsziel der Datenminimierung geht davon aus, dass Daten durch Beratende nur dann erhoben werden, wenn dies für den Beratungsprozess und dessen Verlauf unbedingt erforderlich ist. Dies bedeutet, dass Beratende personenbezogene Daten, wie beispielsweise Kontaktdaten oder Ansprechpartner, nur dann erheben, wenn sie diese für die Beratung benötigen.

Der beste Datenschutz für Ratsuchende ist dann gegeben, wenn möglichst keine beziehungsweise wenige personenbezogene Daten verarbeitet werden. Deshalb sind die Beratenden angewiesen, keine oder nur wenige persönliche Daten von Ratsuchenden zu erheben, zu speichern und zu verarbeiten.

Im Beratungsprozess bedeutet dies, dass Beratende bspw. ärztliche Gutachten, Atteste oder Bescheide von Sozialbehörden nicht für ihre Unterlagen kopieren, sondern diese Dokumente grundsätzlich allein bei den Ratsuchenden verbleiben. Sollte eine Kontaktaufnahme mit einer zuständigen Behörde oder einem Arzt durch die Beratenden notwendig sein, so soll diese im Beisein der Ratsuchenden erfolgen, so dass die notwendigen Legitimationskennzeichen (Bearbeitungsnummer, Aktenzeichen, Versicherungsnummer) ausschließlich bei den Ratsuchenden verbleiben. Bei allen Phasen des Beratungsprozesses haben die Beratenden zu hinterfragen, ob sie die persönlichen Daten tatsächlich für ihre Beratung benötigen.

2. Verfügbarkeit

Verfügbarkeit setzt voraus, dass die personenbezogenen Daten ordnungsgemäß verwendet und gefunden werden können, wenn sie erhoben worden sind. Dies bedeutet die konkrete Auffindbarkeit der Daten (z.B. mit Hilfe von Adressverzeichnissen, Geschäfts- oder Aktenzeichen).

3. Integrität

Die Integrität bezeichnet das Gewährleistungsziel, dass die erhobenen Daten unversehrt, vollständig und aktuell bleiben.

4. Vertraulichkeit

Das Gewährleistungsziel der Vertraulichkeit setzt voraus, dass keine Person personenbezogene Daten unbefugt zur Kenntnis nehmen kann. Hierbei sind Unbefugte nicht nur Dritte außerhalb der Beratungsstelle, sondern auch Beschäftigte von Dienstleistern oder Personen in der Beratungsstelle, die keinen inhaltlichen Bezug zu dem jeweiligen Beratungsverlauf oder zu den jeweiligen Ratsuchenden haben.

5. Nichtverkettung

Das Gewährleistungsziel der Nichtverkettung stellt klar, dass die personenbezogenen Daten nur dem Zweck der Beratung dienen und hierfür verarbeitet und genutzt werden. Sie dürfen nicht für andere Zwecke verarbeitet und ausgewertet werden. Eine Weiterverarbeitung der personenbezogenen Daten ohne Bezug zum Beratungsfall ist innerhalb der Beratungsstelle ausgeschlossen. Dies soll durch technische und organisatorische Maßnahmen sichergestellt werden. Soweit für die Beratungsstelle ihrerseits Berichtspflichten gegenüber staatlichen Stellen oder Fördermittelgebern bestehen, so haben diese durch Anonymisierungs- und Pseudonymisierungsverfahren zu erfolgen. Hierdurch wird der Datenbestand in dem erforderlichen Umgang angepasst.

6. Transparenz

Die Transparenz als Gewährleistungsziel setzt voraus, dass Ratsuchende, Beratende sowie die zuständigen Datenschutzbeauftragten erkennen können, welche Daten für welchen Zweck in einem Beratungsverfahren erhoben und verarbeitet werden.

7. Intervenierbarkeit

Mit dem Gewährleistungsziel der Intervenierbarkeit soll sichergestellt werden, dass Ratsuchende die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam ausüben können. Die Beratungsstelle ist als verantwortliche Stelle verpflichtet, die entsprechenden Maßnahmen einzuleiten und umzusetzen. Dies ist nur möglich, wenn die Beratungsstelle als verantwortliche Stelle jederzeit in den Verlauf der Datenverarbeitung vom Beginn bis zum Ende, dies bedeutet von der Erhebung bis zur Löschung, eingreifen kann.

8. Grundsatz der Direkterhebung

Der Grundsatz der Direkterhebung gem. § 4 Abs. 2 BDSG besagt, dass personenbezogene Daten bei den Betroffenen zu erheben sind. Die Ratsuchenden sollen wissen, welche Daten wann und wie über sie erhoben, gespeichert und verarbeitet werden. Aus diesem Grunde müssen die Ratsuchenden an diesen Vorgängen mitwirken. Die Mitwirkung kann auch durch Bevollmächtigte erfolgen. Sollte es notwendig sein, dass personenbezogene Daten von einer zeitweilig nicht entscheidungsfähigen und damit mitwirkungsunfähigen Person erhoben werden, so ist die betroffene Person davon unverzüglich zu unterrichten, wenn sie diese Information bewusst entgegennehmen kann.

9. Einwilligung des Ratsuchenden

Wichtigste Voraussetzung für einen rechtmäßigen Umgang mit personenbezogenen Daten ist das Vorliegen einer wirksamen Einwilligung der Ratsuchenden. Die Voraussetzungen der Einwilligung nach § 4a BDSG sind:

- persönlich durch die Ratsuchenden,
- aufgrund freier Willensentscheidung,
- in der Regel schriftlich, es sei denn, dass wegen besonderer Umstände eine andere Form angemessen ist,
- die Ratsuchenden sind über die Datenerhebung rechtzeitig und umfassend zu informieren.

Betrifft die Einwilligung sensible Daten, so muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

V. INFORMATIONEN ÜBER DATENSCHUTZ IN DEN BERATUNGSPHASEN

In Beratungsgesprächen kommt es üblicherweise zu unterschiedlichen Situationen, auf die sich Beratende und Ratsuchende einstellen. Der Beratungsverlauf kann dazu führen, dass die Beratenden personenbezogene Daten erhalten, um die Ratsuchenden angemessen zu informieren, unterstützen und begleiten zu können.

Im Folgenden werden daher die einzelnen Beratungsphasen unter dem Blickpunkt des Datenschutzes aufgeführt.

1. Erstkontakt

Beim Erstkontakt ist der Ratsuchende durch die Beratenden über folgende Punkte aufzuklären:

- Die Beratenden haben eine Verschwiegenheitsverpflichtung abgegeben, sie informieren über den Umfang dieser Verschwiegenheitsverpflichtung.
- Sie informieren den Ratsuchenden über den Datenschutz und die Datenschutzerklärung.
- Die Beratenden benennen einen Stellvertreter oder eine Stellvertreterin namentlich und stellen diese/n persönlich vor.
- Wenn dies erforderlich ist, sollen die Kontaktdaten nach Abgabe der Einwilligung der Betroffenen aufgenommen werden.
- Zum Zwecke der Dokumentation des Beratungsverlaufes und für Statistikzwecke bzw. für eine gute Einarbeitung des Stellvertreters oder der Stellvertreterin im Rahmen einer Vertretung legen die Beratenden eine pseudonymisierte Beratungsdokumentation in der Akte der Ratsuchenden an.
- Bescheide, ärztliche Atteste sowie weitere Schriftstücke oder Dateien mit personenbezogenen Daten inklusive sensibler Daten verbleiben durchgehend und ausschließlich in der Verfügungsgewalt der Ratsuchenden. Sollte die Anfertigungen von Kopien zur Bearbeitung des Sachverhaltes notwendig sein, so ist die Anfertigung von Kopien und die Aufnahme in die Akte nur mit vorheriger Einwilligung der Ratsuchenden zulässig. Die sich auf der Kopie befindlichen Merkmale, die einen Bezug zu einer bestimmten Person herstellen können (Name, Anschrift, Geburtsdatum, Versicherungsnummern, Kennzeichnungsnummern u.a.), sind durch „Schwärzen“ in dem gesamten Dokument unkenntlich zu machen.
- Führen die Beratenden die Beratung mit einer Arbeitsassistenz durch, so sind die Ratsuchenden darauf hinzuweisen, dass eine weitere Person sich mit ihren Daten befasst und diese an dem Beratungsgespräch teilnimmt. Für die Assistenten ist durch die Beratenden die Verschwiegenheit sicherzustellen.

2. Folgekontakt ggf. Begleitung

Die Beratenden informieren die Ratsuchenden darüber, dass sie bei einem Folgekontakt/einer Begleitung (ggf. zu Ämtern u.a.) keine Vertretung für die Ratsuchenden übernehmen. Es werden keine Vollmachten erteilt oder Authentifizierungsdaten zur Kommunikation mit Dritten erhoben.

3. Beendigung der Beratung

Nach Beendigung der Beratung werden die Ratsuchenden darauf hingewiesen, dass die von ihnen vorliegenden persönlichen Dokumente gelöscht bzw. anonymisiert werden, soweit diese nach Ende der Beratung für Zwecke der Statistik und Förderung notwendig sind.

VI. KOMMUNIKATIONSMITTEL UND SICHERHEIT

1. Kommunikation am Telefon
2. Email
3. Persönlich
4. Kontakt über Twitter/Facebook
5. Post

Wichtige Hinweise an Ratsuchende
Die Ratsuchenden sollen und müssen beachten, dass die von ihnen bei der Nutzung dieser Kommunikationswege preisgegebenen persönlichen Daten unterschiedlich gesichert sind.
Grundsätzlich soll bei der ersten Kontaktaufnahme nur der Austausch der Kontaktdaten und mithin der personenbezogenen Daten wie Name, Anschrift, Telefonnummer, Emailadresse notwendig sein.

Bitte sehen Sie als Ratsuchende davon ab, der Beratungsstelle bereits bei der ersten Kontaktaufnahme Bescheide, ärztliche Atteste oder eine komplette schriftliche/textliche Schilderung Ihres derzeitigen Gesundheitszustandes auf analogem oder digitalem Weg zukommen zu lassen. Wir empfehlen keine Originaldokumente und Bescheide einzureichen und zu überlassen.

Zu den einzelnen Möglichkeiten der Kontaktaufnahme sind folgende Hinweise notwendig:

1. Telefon

Grundsätzlich haben die Beratenden bei jedem Telefonat dafür Sorge zu tragen, dass die Gespräche mit den Ratsuchenden nicht von unberechtigten Dritten mitgehört werden können. Dies bedeutet, dass das Telefonat von den Beratenden zwingend in einem vor fremden Zuhörern geschützten Raum stattzufinden hat. Im Umkehrschluss ist auch den Ratsuchenden anzuraten, dass diese Telefonate mit den Beratenden nicht in öffentlichen Bereichen (Park, Café, Zug, Supermarkt etc.) geführt werden. Um dies zu unterstützen, werden die Beratenden zu Beginn eines jeden Telefonates erfragen, ob die Ratsuchenden sich an einem für das Telefonat geeigneten Ort aufhalten.

1.1. Erstkontakt zur Vereinbarung eines persönlichen Besprechungstermins

Bei der Kontaktaufnahme via Telefon zum Zwecke der Vereinbarung eines Beratungsgespräches können die Beratenden von Ratsuchenden den Namen und die Kontaktdaten aufnehmen. Soweit Ratsuchende ihre Kontaktdaten ungefragt äußern und um eine Rückmeldung bitten, handelt es sich um eine unaufgeforderte Mitteilung. Eine solche Mitteilung ist als Einwilligung im Sinne des § 4 BDSG zur Erhebung der persönlichen Daten durch die Beratungsstelle zu qualifizieren. Die Beratenden sollten dennoch die Ratsuchenden hierauf hinweisen und explizit erfragen, ob sie dieser Datenverarbeitung durch die Beratungsstelle zustimmen.

Kontaktdaten sind: Name, Vorname, Anschrift, Telefonnummer, Emailadressen.

Weitere Daten werden die Beratenden während der ersten Kontaktaufnahme zu Vereinbarung eines Besprechungstermins nicht erheben.

Bei der ersten telefonischen Kontaktaufnahme können die Ratsuchenden den Beratenden bereits umreißen, um welche Fragestellung es sich handelt und wie ihre persönliche Situation aussieht. Hierüber werden die Beratenden sich keine Aufzeichnungen machen.

Die Beratenden werden den Ratsuchenden über die unter V.1. stehenden Punkte informieren.

1.2. Erstkontakt mit Beratung am Telefon

Findet eine Kontaktaufnahme per Telefon statt und schließt sich direkt ein telefonisches Beratungsgespräch an, so haben die Beratenden die Ratsuchenden grundsätzlich über die unter V.1. genannten Punkte zu unterrichten.

Die Beratenden werden sich in dem Beratungsgespräch nur solche Aufzeichnung machen, die für die Beantwortung der Fragen der Ratsuchenden notwendig sind.
Wenn kein Folgekontakt vereinbart wurde, werden die Beratenden keine Kontaktdaten der Ratsuchenden aufnehmen und auch keine weiteren persönlichen Daten der Ratsuchenden im Sinne des BDSG erheben, speichern oder verarbeiten.

1.3. Folgekontakte am Telefon

Sollte es sich klar abzeichnen, dass über die erste Kontaktaufnahme hinaus eine Begleitung stattfindet und die Beratung andauert, so werden sich Beratende und Ratsuchende auf ein Kennwort zur Authentifizierung

einigen. Dieses wird auch dem Stellvertreter oder der Stellvertreterin der Beratenden bekannt gegeben.

2. Email

Soweit die Ratsuchenden sich per Email direkt oder über das Kontaktformular der Webseite der Beratungsstelle mit dieser in Verbindung setzen, werden die Ratsuchenden darauf hingewiesen, dass sie der Beratungsstelle keine Bescheide, Anträge oder andere Formulare mit sensiblen Daten über ihren Gesundheitszustand als Anhänge übersenden.

Des Weiteren sollten die Ratsuchenden darauf achten, dass sie in ihrer Email, soweit eine unverschlüsselte Übertragung erfolgt, keine sensiblen Gesundheitsdaten über sich preisgeben, da die Gefahr besteht, dass die Email an den falschen Adressaten gesendet wird oder auf dem Weg zum Empfänger über eine Versendung im Internet auf nicht sicherem Übertragungsweg von dritten Unberechtigten gelesen werden kann.

Diesen ersten Hinweis hat die Beratungsstelle bereits auf ihrer Webseite vermerkt, und sie wird die Ratsuchenden auch im Falle einer ersten Kontaktaufnahme via Email darauf hinweisen.

Für den Fall, dass die Ratsuchenden unaufgeforderte Dokumente als Anhänge übersenden, die nunmehr in den Zugriffsbereich der Beratenden gelangt sind, werden sie die Ratsuchenden auf diesen Umstand hinweisen und sodann mit diesen gemeinsam eine Löschung der übersandten Dokumente durchführen, soweit diese für die Beratungstätigkeit der Beratenden nicht unbedingt erforderlich sind.
Sind die übersandten Dokumente für die weitere Beratung notwendig, so sind die personenbezogenen Daten, soweit dies möglich ist, in den Dokumenten unkenntlich zu machen. Die Beratenden werden die Ratsuchenden über die unter V.1. stehende Punkte informieren.

Die Beratung per Email kann nur dann sicher ohne eine Verschlüsselung durchgeführt werden, wenn keine personenbezogenen Daten in den Nachrichten enthalten sind. Ist dies nicht möglich, so sind die Nachrichten zu verschlüsseln.

3. Persönlich in der Beratungsstelle

Suchen die Ratsuchenden persönlich die Beratungsstelle auf, ist durch die Beratenden sicherzustellen, dass das Gespräch vertraulich stattfindet. Die Beratenden werden in der ersten Beratungssituation persönlich den Ratsuchenden eine Einwilligungserklärung im Sinne dieses Datenschutzhandbuches übergeben und diese auch über die Datenschutzerklärung und den Datenschutz hinweisen sowie ihnen eine ausgedruckte Version der Datenschutzerklärung oder auf Wunsch eine elektronische Version (barrierefreie PDF) übersenden, so dass diese ohne weitere Barrieren die Möglichkeit haben, sich über die Datenschutzerklärung und das Datenschutzhandbuch zu informieren.
Es wird empfohlen, dass die Beratungsstelle die Datenschutzbestimmungen des Datenschutzhandbuches sichtbar auf ihrer Internetseite zugänglich macht.

Soweit sich an die erste Kontaktaufnahme in der Geschäftsstelle direkt ein Beratungsgespräch anschließt, haben die Beratenden, sofern dies möglich ist, bereits in diesem Treffen ihren ständigen Vertreter oder ihre ständige Vertreterin vorzustellen.

Auch hier ist zu beachten, dass diesen gegenüber ebenso eine datenschutzrechtlich relevante Einwilligung abgegeben wird. Erscheinen die Ratsuchenden in Begleitung und sind Kontaktdaten von der Begleitperson als Ansprechpartner notwendig, ist von der Begleitperson eine datenschutzrechtlich relevante Einwilligung für die Speicherung, Erhebung und Verarbeitung sowie Nutzung der personenbezogenen Daten in Bezug auf die Kontaktaufnahme notwendig.
In dem Beratungsgespräch sind die Ratsuchenden sowie deren Begleitung darauf hinzuweisen, dass die Beratenden als auch deren ständige Vertretung eine Verschwiegenheits- und Neutralitätsverpflichtung gegenüber der Beratungsstelle abgegeben haben.

Sie weisen ausdrücklich die Ratsuchenden darauf hin, dass die Gesprächsinhalte im Rahmen des Beratungsprozesses nicht an Dritte weitergegeben werden und vor dem Zugriff unberechtigter Dritter geschützt werden, soweit personenbezogene Daten aufgenommen werden.

Die Beratenden werden die Ratsuchenden über die unter V.1. stehende Punkte informieren.

4. Twitter und Facebook

Bei der Kontaktaufnahme über Twitter und Facebook ist zu berücksichtigen, dass es sich um öffentliche Plattformen handelt. Wenn die Ratsuchenden keine Direktnachrichten schicken, sind die Nachrichten, welche sie an die Beratungsstelle versenden, für alle zugänglich, lesbar und nur beschränkt wieder aus dem Internet löschbar.

Die Ratsuchenden werden dringend darum gebeten, davon abzusehen, sensible Daten ihrerseits zu veröffentlichen. Auch die Kommunikationswege über Twitter und Facebook mittels einer Direktnachricht über die Anwendung sind keine sicheren Verfahren. Es handelt sich hierbei um Unternehmen, die ihren Sitz in Irland bzw. den USA haben. Die Datenströme werden an diese Länder geleitet, so dass hier andere datenschutzrechtliche Bestimmungen gelten.

Die Sicherheit dieser sensiblen Daten wird von den Unternehmen nicht gewährleistet.
Den Beratenden ist es untersagt, auf diesem Wege Beratung durchzuführen oder sensible Daten der Ratsuchenden auszutauschen.

Der Kommunikationsweg über Twitter und Facebook soll lediglich als Möglichkeit der ersten Kontaktaufnahme benutzt werden.

5. Post

Die Ratsuchenden sollten davon absehen, eine Postkarte an die Beratungsstelle zu übersenden, in welcher sie persönliche oder sensible Daten preisgeben. Die Postkarte ist unverschlossen für unbefugte Dritte lesbar.

Soweit die Kontaktaufnahme per Post durch einen verschlossenen Brief erfolgt, bitten wir davon Abstand zu nehmen, Kopien von Anträgen oder Dokumenten mit persönlichen sensiblen Gesundheitsdaten oder anderen Daten an die Beratungsstelle zu übersenden. Auch wenn es sich hier gemäß Art. 10 GG – aufgrund des vorliegenden Postgeheimnisses – um einen der sichersten Übertragungswege handelt, ist die Beratungsstelle nicht dazu befugt, solche Unterlagen zu erheben, zu speichern und zu nutzen, soweit dies nach den datenschutzrechtlichen Bestimmungen der Bundesrepublik Deutschland und des vorliegenden Datenschutzhandbuches nicht unbedingt für den Beratungsprozess erforderlich ist.

Sollte eine Übersendung erfolgt sein, so wird in dem dann folgenden Beratungsgespräch mit den Ratsuchenden erläutert, ob die Unterlagen notwendig sind. Sollte dies nicht der Fall sein, werden die Unterlagen im Beisein der Ratsuchenden unwiederbringlich vernichtet oder diesen wieder übergeben.

Sollte es für die Beratung erforderlich sein, dass Bescheide und weitere Dokumente mit sensiblen Daten der Ratsuchenden von den Beratenden für die Beratung benötigt werden, so sind eine persönliche Übergabe oder eine Übersendung per Post im verschlossenen Brief sichere Übertragungswege.

VII. ELEKTRONISCHE AKTEN, AKTENZEICHEN, DOKUMENTENMANAGEMENT UND ANONYMISIEREN UND BERECHTIGUNGEN

Die Beratenden werden zur Durchführung ihrer Beratungsarbeit und der Beratung elektronische Akten wie folgt führen.

1. Elektronische Akte

Die Akten werden durch die Beratenden ausschließlich elektronisch geführt. Dies bedeutet, dass eine physische Papierakte nicht angelegt und geführt wird. Die Dokumente und persönlichen Daten werden ausschließlich elektronisch auf dem Arbeitsrechner sowie dessen Systemsicherung der Beratenden erfasst und geführt. Papierakten dürfen nicht geführt werden. Der Ordner ist mit einem Passwort zu schützen.

2. Vergabe eines Aktenzeichens

Für jede Anfrage, egal auf welchem Kommunikationsweg und von welcher Dauer, werden die Beratenden eine Aktennummer vergeben. Die Aktennummer beginnt am 01. Januar eines jeden Jahres mit einer fortlaufenden Nummerierung entsprechend des Eingangs der Beratungsanfrage. (Beispielsweise 1-17; 2-17; ...; 233-17).

3. Dokumentenmanagement

Die Beratenden erstellen auf ihrem Arbeitsplatzrechner einen Ordner mit der für die Beratung vergebenen Aktennummer (Ordner 1-17).

Die Beratenden hinterlegen sodann in einem Textdokument die Kontaktdaten und Ansprechpartner für diese Beratung und speichern diese Textdatei als Kontaktdaten 1-17 in dem Ordner des Aktenzeichens 1-17 ab.

Die Beratenden erstellen ein Textdokument als „Logbuch". In diesem Logbuch sind der Verlauf der Beratung und Telefonnotizen/Kommunikation einzustellen. In diesem Dokument werden die Ratsuchenden nicht mit persönlichem Namen oder persönlichen Daten benannt. Sie werden ausschließlich als Ratsuchende bezeichnet.
Alle Dokumente, welche die Beratenden im Laufe ihrer Beratungstätigkeit erhalten und die für ihre Arbeit notwendig sind, werden diese als PDF in dem Ordner speichern. In den PDF sind alle personenbezogenen Angaben unkenntlich zu machen („zu schwärzen").
An die Beratenden versandte Emails und von diesen an die Ratsuchenden verschickte Nachrichten sind in einem Unterordner (Email Korrespondenz 1-17) als PDF zu speichern. In der PDF sind alle personenbezogenen Daten der Ratsuchenden unkenntlich zu machen.

In die Aktendokumentation ist die Einwilligungserklärung der Ratsuchenden als Scan mit aufzunehmen. Das Original der Einwilligung in Papierform wird in einem Ordner „Einwilligungen" verschlossen aufbewahrt.

4. Anonymisieren

Bei Beendigung der Beratung ist in dem Ordner (der elektronischen Akte) die Textdatei mit den Kontaktdaten unwiederbringlich zu löschen. Die Akte darf nunmehr keine personenbezogenen Daten der Ratsuchenden erhalten. Die Beratenden prüfen die einzelnen Dokumente auf diese Voraussetzung. Nach erfolgter Prüfung und ggf. Unkenntlichmachung ändern die Beratenden den Namen des Ordners um von „1-17" in „1-17archviert23.07.2017" um. Die Beratenden können sich hierbei einer Verwaltungshilfe/Arbeitsassistenz bedienen, wenn diese ebenso der Verschwiegenheitsverpflichtung unterliegt.

VIII. MASSNAHMEN ZUR SICHERUNG DES DATENSCHUTZES

Maßnahmen des Datenschutzes sind solche, die den Zutritt, Zugang und Zugriff auf die personenbezogenen Daten einschränken. Die personenbezogenen Daten dürfen nur von den Berechtigten erhoben, verwaltet und verarbeitet werden.

1. Beratungsstelle

Die Räume in der Beratungsstelle sind so zu gestalten, dass ein vertrauliches Gespräch ohne das Mithören des Gesprächs durch Dritte möglich ist. Die Räume der Beratungsstelle, in denen personenbezogene Daten aufbewahrt werden, sind vor dem unberechtigten Zutritt Dritter zu sichern. Die Beratenden haben Sorge dafür zu tragen, dass sich unberechtigte Dritte nicht unbeaufsichtigt in den Räumen der Beratungsstelle aufhalten.

2. Einsatz von Informationstechnologie

Alle Beratenden haben im Rahmen ihrer Tätigkeit, soweit diese elektronische Datenverarbeitung (EDV) durch die Anwendung von Desktoprechnern, Laptops, Smartphones, Tablets benutzen, dafür Sorge zu tragen, dass die dort gespeicherten personenbezogenen Daten passwortgeschützt und gesichert sind.

Personenbezogene Daten der Ratsuchenden müssen weiterhin auffindbar auf dem Computer der Beratenden entsprechend der oben aufgeführten Aktenstruktur gespeichert bzw. archiviert werden. Es dürfen keine Parallelakten oder doppelte Dateien vorhanden sein. Wurde ein Dokument erfolgreich in die Akte überführt, so ist das ursprüngliche elektronische Dokument zu löschen (Scan im Scanordner, E-Mail im E-Mail-Programm).

Die Beratenden haben bei der Nutzung von IT sämtliche Sicherheitsvorkehrungen und Passwortrichtlinien zu beachten. Insbesondere haben sie auf den von ihnen genutzten Computern sicher zu stellen, dass die Antivirensoftware jeweils auf dem aktuellen Stand ist. Darüber hinaus haben sie sicher zu stellen, dass eine Datenübermittlung an Dritte nicht stattfinden kann.

Personenbezogene Daten dürfen nicht auf externen Datenträgern wie USB-Sticks, CDs oder anderen mobilen Datenträgern gespeichert werden, mit einer Ausnahme:

die Anfertigung einer Sicherungskopie zum Zwecke der Datensicherung (siehe hier unter Punkt: VIII.4.). Die Beratenden werden ausschließlich solche Softwareprogramme zur Verarbeitung der Daten benutzen, die ausschließlich auf dem Computer bzw. dem festen Arbeitsplatz der Beratenden installiert sind.
Cloud-Dienste dürfen nicht genutzt werden.

Soweit mobile Datenträger im Einsatz sind (Laptop, Tablet, Smartphone), haben die Beratenden stets das Gerät unter Verschluss zu halten und vor Diebstahl zu sichern. Die Beratenden sollen auf mobilen Endgeräten wie Tablets und Smartphones nur diejenigen Daten speichern, die auch unbedingt benötigt werden. Ein Passwortschutz des Gerätes ist zwingend notwendig. Soweit mit diesen mobilen Datenträgern Email-Kommunikation mit den Ratsuchenden durchgeführt wird, die parallel auch auf dem Arbeitsplatzrechner vorhanden ist, so sind die Emails auf dem Tablet und dem Smartphone nach Bearbeitung unverzüglich zu löschen. Sind die mobilen Geräte in der Beratungsstelle zu verwahren, so sind diese sicher zu verschließen.

Die Beratenden werden bei der Nutzung des Internets stets darauf achten, dass sie im Netz sicher surfen und keine dubiosen Seiten aufrufen, welche einen Angriff auf den Computer ausüben, um Daten auszuspähen oder zu zerstören.

Bei der Nutzung der Email-Kommunikation ist stets auf eine sichere Kommunikation zu achten. Dies bedeutet, dass Emails mit einer Ende-zu-Ende-Verschlüsselung an den Empfänger versandt werden. Ebenso ist vor Absenden der Email nochmals der Adressat zu prüfen. An der Email hat eine Signatur darauf hinzuweisen, dass unberechtigte Dritte die Nachricht unverzüglich löschen und den Absender darüber informieren, dass die Email fehlgeleitet wurde. Es ist den Beratenden grundsätzlich nur gestattet, an verifizierte Emailadressen Nachrichten zu versenden.
Unverschlüsselte sensible Daten dürfen nicht per Email versandt werden. Siehe IV.2.

3. Passwörter

Bei der Vergabe von Passwörtern ist darauf zu achten, dass diese nach den Empfehlungen des Bundesamtes für Sicherheit und Informationstechnik zu erstellen sind.

- Das Passwort muss mindestens 8 Zeichen lang sein, wobei Buchstaben, Ziffern und Sonderzeichen enthalten sein sollten.

Folgendes ist im Weiteren zu beachten:

- Verwenden Sie keine Namen, ändern Sie das Passwort regelmäßig.
- Schreiben Sie das Passwort nicht auf.
- Verwenden Sie unterschiedliche Passwörter.
- Ändern Sie voreingestellte Passwörter.
- Sichern Sie auch den Bildschirmschoner mit einem Kennwort.

4. Datensicherung

Eine Datensicherung hat in regelmäßigen Abständen zu erfolgen. Die Datenbank der Beratungsfälle soll durch den Anschluss und das Überspielen der Ordner auf eine externe Festplatte gesichert werden. Der Zugriff auf die Daten auf der externen Festplatte ist durch ein Passwort zu sichern. Die externe Festplatte darf nicht aus dem Raum der Beratungsstelle entfernt werden und ist dort verschlossen und sicher aufzubewahren. Bei der Datensicherung ist sicherzustellen, dass der Ordner jeweils in seiner aktuellen Version überschrieben wird. Es dürfen sich auf der Festplatte nicht mehrere Beratungsordner unterschiedlichen Datums befinden. So soll vermieden werden, dass eine Anonymisierung nicht stattfinden kann, da die personenbezogenen Daten immer noch nicht anonymisiert durch eine frühere Sicherungskopie vorhanden sind. Eine anderweitige Sicherung auf einem Server oder durch Cloud-Dienste ist unzulässig.

5. Vorgehensweise bei einer Datenpanne

Unter einer Datenpanne (Data Breach) versteht man die ungewollte Preisgabe von an sich verschlossenen personenbezogenen Daten, die zu einem Verstoß gegen die Datensicherheit und den Datenschutz führt. Eine Datenpanne kann unterschiedliche Ursachen haben: bspw. ein Ausspähen der Daten durch einen Hackerangriff, Datenverlust, Datendiebstahl, falsche Versendung an falsche Emailadressen.

Für den Fall, dass die Beratenden oder in der Beratungsstelle verantwortliche Personen oder andere Dritte von einer Datenpanne Kenntnis erlangen, werden sie den Betroffenen unverzüglich, also ohne schuldhaftes Zögern, hierüber informieren. Dies ungeachtet von einer

vorherigen Abwägung, wie schwerwiegend die Beeinträchtigung für die Rechte oder die schutzwürdigen Interessen der Betroffenen sind. Sie werden auch mit der zuständigen Aufsichtsbehörde, den Landesdatenschutzbeauftragten Kontakt aufnehmen.

Von einer Benachrichtigung der Betroffenen ist dann abzusehen, wenn angemessene Maßnahmen zur Sicherung der Daten noch ergriffen werden müssen oder aber eine vorherige Information der Betroffenen zu einer Gefährdung der Strafverfolgung führen würde. Den Betroffenen ist sodann umfassende Mitteilung zu machen, welche Daten von ihnen in welchem Ausmaß preisgegeben wurden.

6. Berechtigungen

Berechtigt zum Umgang mit den persönlichen Daten der Ratsuchenden sind allein die Beratenden und deren Stellvertreter oder Stellvertreterin.
Zu Stellvertreter bzw. Stellvertreterin siehe unter: X.

IX. RECHTE DES RATSUCHENDEN

Dem/Der Ratsuchenden stehen nach dem Bundesdatenschutzgesetz als Betroffene Rechte zu.

1. Benachrichtigung gemäß § 33 BDSG

Die Ratsuchenden sind darüber zu benachrichtigen, wenn von Ihnen durch die Beratungsstelle personenbezogene Daten erstmals gespeichert oder übermittelt werden. Die Beratenden werden die Ratsuchenden, sollten diese nicht bei der erstmaligen Datenerhebung anwesend sein, in Textform hierüber benachrichtigen.

2. Auskunftsrecht gemäß § 34 BDSG

Die Beratungsstelle hat den Ratsuchenden Auskunft zu erteilen über die zu ihrer Person gespeicherten Daten, wenn es verlangt wird. Die Auskunft ist zu erteilen über:

- die zu ihrer Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
- den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und
- den Zweck der Speicherung.

3. Berichtigung, Löschung und Sperrung der Daten gemäß § 35 BDSG

Der/Die Ratsuchende hat ein Recht, dass unrichtige gespeicherte Daten berichtigt werden. Der/Die Ratsuchende hat ein Recht auf Löschung.

Personenbezogene Daten sind zu löschen, wenn

- ihre Speicherung unzulässig ist,
- es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,
- sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, oder
- sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten Jahres ergibt, dass eine länger währende Speicherung nicht erforderlich ist. Soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widerspricht, können die Daten bereits am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgt, gelöscht werden.

Sollten der Löschung gesetzliche, satzungsgemäße oder vertragliche Aufbewahrungsfristen entgegenstehen, so sind die Daten zu sperren. Mit der Sperrung wird erreicht, dass die Daten zwar noch vorhanden sind, sie aber nicht mehr genutzt werden dürfen und somit über diese Daten nicht verfügt werden darf.

X. STELLVERTRETER

Die Beratenden haben den Ratsuchenden ihren Stellvertreter oder ihre Stellvertreterin zu benennen, vorzustellen und deren Kontaktdaten an die Ratsuchenden zu senden. Die Ratsuchenden sind zu informieren, sollten die Beratenden erkrankt oder urlaubsbedingt außer Dienst sein.
Die Beratenden haben ihrem Stellvertreter oder ihrer Stellvertreterin Zugang zu den Beratungsakten zu verschaffen. Die Email-Kommunikation wird im Zeitraum der Abwesenheit ausschließlich über die E-Mail des Stellvertreters oder der Stellvertreterin geführt. Die Beratenden richten eine Abwesenheitsbenachrichtigung und eine Mitteilung der Kontaktdaten ihres Stellvertreters oder ihrer Stellvertreterin ein. Die Daten dürfen von den Beratenden zu dem Stellvertreter oder der Stellvertreterin nicht durch Übersendung im Netzwerk oder im Internet übertragen werden. Die Sicherungsfestplatte ist das einzige zulässige Übertragungsmedium. Dies nur für den Fall, dass beide Beratende nicht den gleichen PC/Arbeitsplatz benutzen.

XI. GLOSSAR

A

Akte
Eine digitale oder analoge Akte ist der Zusammenschluss mehrerer Dokumente (elektronisch oder in Papierform) in Bezug auf einen bestimmten Vorgang, wobei die Dokumentensammlung einem bestimmten Aufbau folgt und für mehr als einen Vorgang angewendet wird.

Anonymisierung
Anonymisierung im Sinne des Bundesdatenschutzgesetzes ist die vollständige- und rücknahmefeste Trennung von einer Person und deren Daten. Ziel der Anonymisierung ist es, dass aufgrund der Daten nicht mehr auf eine Person geschlossen werden kann, so dass im Sinne des Bundesdatenschutzgesetzes keine persönlichen Daten mehr vorliegen.

Aufsichtsbehörde
Die Aufsichtsbehörde kontrolliert die Ausführung u.a. des Bundesdatenschutzgesetzes sowie der Landesdatenschutzgesetze, denen die Aufsichtsbehörden für den Datenschutz jeweils unterstellt sind. Die Tätigkeitsberichte der Bundes- und der Landesdatenschutzbeauftragten und der Aufsichtsbehörde für den Datenschutz sind in dem Zentralarchiv für Tätigkeitsberichte der Bundes- und der Landesdatenschutzbeauftragten der Aufsichtsbehörden für Datenschutz ab dem Jahre 2014 veröffentlicht (www.thm.de/zaftda).

Auftragsdatenverarbeitung
Eine Auftragsdatenverarbeitung im Sinne des Datenschutzrechts liegt dann vor, wenn personenbezogene Daten durch einen Dienstleister, der so genannten verantwortlichen Stelle, erhoben, verarbeitet oder genutzt werden. Gemeint ist, dass ein Unternehmen oder ein Verein, das oder der Daten erhebt, speichert, verarbeitet und an einen externen Dienstleister, bspw. ein Callcenter, eine Abrechnungsstelle oder für Wartungsarbeiten weitergibt.

B

Betroffene
Bei dem oder der Betroffenen handelt es sich um eine bestimmte oder bestimmbare natürliche Person, deren Daten datenschutzrechtlich relevant verarbeitet werden.

Berechtigungen
Berechtigt zur Einsichtnahme der personenbezogenen Daten der Ratsuchenden sind allein die Beratenden der Beratungsstelle. Andere Personen dürfen keinen Zugriff auf die personenbezogenen Daten haben.

Big Data
Big Data ist die automatisierte Auswertung von digitalen Datenmengen.

Bundesdatenschutzgesetz
Das Bundesdatenschutzgesetz der Bundesrepublik Deutschland vom 01.02.1977 regelt die Grundsätze und den Umgang mit personenbezogenen Daten in der Bundesrepublik Deutschland. Das Bundesdatenschutzgesetz wurde reformiert, nachdem im Jahre 2016 die Datenschutzgrundverordnung der Europäischen Union verabschiedet wurde.

C

Cloud Computing
Unter Cloud Computing wird die Speicherung, die Nutzung von Rechenleistung oder eine Anwendungssoftware als Dienstleistung über das Internet verstanden. Die Daten werden somit nicht mehr auf dem lokalen Rechner gespeichert, verarbeitet und genutzt, sondern über das Internet verarbeitet. Bspw. redet man von Cloud Computing, wenn es um die Speicherung von großen Datenmengen auf externen Speicherplätzen wie etwa OneNote oder Dropbox sowie von einer Anwendung von Software nur über den Desktop wie bspw. Word 365 als Desktopversion geht.

Computerviren
Unter dem Begriff Computerviren versteht man ein Programm, welches andere Computerprogramme und Betriebssysteme schädlich ändert, so dass Daten gestohlen oder zerstört werden. Unter dem großen Begriff des Computervirus versteht man so genannte Malware, Computerwürmer und trojanische Pferde.

D

Datei
Unter einer Datei wird eine Sammlung von Daten, die in einem gewissen inneren und äußeren Zusammenhang stehen, verstanden. Eine Datei kann demzufolge auch eine Akte sein.

Datenschutzbeauftragte
Beauftragte für die Sicherung und Wahrung des Datenschutzes sind Aufsichtsgremien innerhalb privater Unternehmen bzw. öffentlicher Behörden innerhalb der Bundesrepublik Deutschland, soweit es um die Aufsichtsbehörden des Bundesdatenschutzrechts geht. Unternehmen und öffentliche Stellen haben die Verpflichtung, Datenschutzbeauftragte zu bestellen, wenn eine gewisse Anzahl von Mitarbeitern bzw. eine bestimmte Art der Datenbearbeitung durchgeführt wird.
Eine Bestellung eines oder einer Datenschutzbeauftragten kann auch erfolgen, soweit diese gesetzlich vorgeschrieben ist. Der oder die Datenschutzbeauftragte ist grundsätzlich weisungsunabhängig und hat die Aufgabe, die Vorgänge in dem Unternehmen bzw. der Behörde datenschutzrechtlich zu prüfen. Er oder sie ist Ansprechpartner für Personen, deren personenbezogene Daten von dem Unternehmen bzw. der öffentlichen Stelle erhoben, verarbeitet oder genutzt werden.

Datenpanne
Unter einer Datenpanne (Data Breach) versteht man die ungewollte Preisgabe von an sich verschlossenen personenbezogenen Daten, die zu einem Verstoß gegen die Datensicherheit und den Datenschutz führen. Eine Datenpanne kann unterschiedliche Ursachen haben, bspw. ein Ausspähen der Daten durch einen Hackerangriff, Datenverlust, Datendiebstahl, falsche Versendung an falsche Emailadressen.

Datengeheimnis
Unter dem Datengeheimnis ist nach dem Bundesdatenschutzrecht der Bundesrepublik Deutschland die Pflicht zu verstehen, dass bei der Datenverarbeitung Beschäftigte personenbezogene Daten unbefugt nicht erheben, verarbeiten oder nutzen dürfen. Private Unternehmen müssen ihre Mitarbeiter bei Aufnahme ihrer Tätigkeit auf das Datengeheimnis verpflichten.

Datenvermeidung und Datensparsamkeit
Unter diesen Begriffen versteht man ein Gewährleistungsprinzip des deutschen Datenschutzrechts. Dieses Schutzziel ist auch in der Europäischen Datenschutzgrundverordnung verankert und meint eine wesentliche Säule des Datenschutzrechts, nämlich den Grundsatz, dass Daten nur dann erhoben, verarbeitet und genutzt werden sollen, wenn dies zur Erreichung eines bestimmten Zweckes unbedingt erforderlich ist.

E

Einsichtsrecht
Betroffene haben nach dem Datenschutzrecht der Bundesrepublik Deutschland grundsätzlich gegenüber denjenigen, den so genannten verantwortlichen Stellen, die von ihnen Daten erheben, speichern oder nutzen, das Recht und den gerichtlich durchsetzbaren Anspruch auf Auskunft und Einsicht ihrer Daten.

Einwilligung
Unter Einwilligung im Sinne des Bundesdatenschutzgesetzes versteht man die vorherige Abgabe einer so genannten Willenserklärung, dass die Verarbeitung, Erhebung und Nutzung von personenbezogenen Daten für den vorgegebenen Zweck erfolgen kann und hiergegen keine Einwendungen erhoben werden. Die Einwilligung hat gemäß § 4a Bundesdatenschutzgesetz grundsätzlich schriftlich zu erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Die Einwilligung ist jederzeit widerrufbar und muss auf einer freien Entscheidung der Betroffenen beruhen.

G

Gesundheitsdaten
Gesundheitsdaten sind gemäß § 3 Abs. 9 Bundesdatenschutzgesetz besonders sensible Daten. Sie bedürfen eines besonderen Schutzes. Gesundheitsdaten sind u.a. individuelle medizinische Informationen einer bestimmten natürlichen Person. Es sind alle Daten, die den physischen und psychischen Zustand von Menschen betreffen und die im Zuge einer medizinischen Betreuung, Untersuchung, Pflege erhoben werden und zur Verrechnung von Gesundheitsdienstleistungen bzw. der Versicherung von Gesundheitsrisiken dienen.
Gesundheitsdaten, als besonders sensible Daten, dürfen keinesfalls unverschlüsselt per Email an Dritte versandt werden.

I

Informationelle Selbstbestimmung
Das Recht auf informationelle Selbstbestimmung ist eine Ausprägung des allgemeinen Persönlichkeitsrechts und wurde durch das Bundesverfassungsgericht im so genannten Volkszählungsurteil (BVerfG, BVerfGE 65, 1) anerkannt. Es ergibt sich aus Artikel 2 Abs.1 in Verbindung mit Artikel 1 Abs. 1 Grundgesetz.

Unter dem Recht der informationellen Selbstbestimmung versteht man das Recht jedes Einzelnen, für sich selbst über seine personenbezogenen Daten zu bestimmen und festzulegen, wie bzw. wem diese gegenüber preisgegeben und von wem diese verarbeitet werden.

L

Löschen
Löschen ist gemäß § 3 Abs. 4 Nr.5 Bundesdatenschutzgesetz das Unkenntlichmachen von Daten. Dies bedeutet, dass durch eine Handlung die Daten irreversibel zerstört werden. Hierfür sind besondere technische Möglichkeiten gegeben.

N

Natürliche Person
Der Schutz personenbezogener Daten bezieht sich ausschließlich auf Daten von natürlichen Personen. Natürliche Personen sind Menschen, die rechtsfähig sind. Gemäß § 1 BGB beginnt die Rechtsfähigkeit des Menschen mit Vollendung der Geburt. Unter dem Begriff der Rechtsfähigkeit ist juristisch die Fähigkeit zu verstehen, selbst Träger von Rechten und Pflichten zu sein. Nur eine rechtsfähige Person kann selbst Ansprüche geltend machen und hat im Rechtsgefüge Verpflichtungen einzuhalten. Die Rechtsfähigkeit endet mit dem Tod des Menschen. Wann der Tod eingetreten ist, wird von der Rechtsnorm als naturwissenschaftlich feststehend und daher als nicht regelungsbedürftig angesehen. Das Gesetz orientiert sich somit an dem jeweiligen Fortschritt der Medizin und an dem jeweiligen medizinischen Begriff. Nach derzeitigem Erkenntnisstand ist von dem Tod eines Menschen auszugehen, wenn die Gesamtfunktion des Großhirns, Kleinhirns und Hirnstamms endgültig und nicht behebbar ausgefallen ist und dauerhaft keine Gehirnkurven mehr geschrieben werden können.

P

Pseudonymisierung
Der Begriff des Pseudonyms steht für einen erfundenen Namen. Diesen, seine Identität verdeckenden, Namen können sich Betroffene selbst geben. Er kann ihnen aber auch von einem Dritten zugewiesen sein. Dies kann mit oder ohne Information der Betroffenen geschehen. Auch verschlüsselte Daten sind pseudonymisierte personenbezogene Daten. Die Pseudonymisierung hat das Ziel, die unmittelbare Kenntnis der vollen Identität der Betroffenen während Bearbeitungs- und Nutzungsvorgängen, bei denen der Personenbezug nicht zwingend erforderlich ist, auszuschließen. Die Pseudonymisierung ist nicht gleichzusetzen mit der Anonymität.
Die Beratenden verfügen über eine entsprechende Referenzdatei, mit deren Hilfe das Pseudonym aufgelöst werden kann.

S

Sammlung
Eine Sammlung ist eine absichtlich zusammengetragene oder aufrecht erhaltene Mehrheit von Daten, die untereinander in einem Zusammenhang stehen. Die Datensammlung kann über eine einzelne Person oder über eine Vielzahl von Personen mit demselben Merkmal erfolgen.

Sozialdaten
Sozialdaten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener oder Betroffene), die von einer Behörde im Rahmen des Sozialverwaltungsverfahrens erhoben, verarbeitet oder genutzt werden.

Sperrung
Unter einem Sperren ist das Kennzeichnen personenbezogener Daten zu verstehen, um ihre weitere Verarbeitung oder Nutzung einzuschränken.

Stellvertreter
Die Beratenden der jeweiligen Beratungsstelle werden bereits beim Erstkontakt ihren Stellvertreter oder ihre Stellvertreterin benennen. Diese sind den Ratsuchenden im Rahmen des Beratungsverlaufes, sollten sich Folgeberatungen ergeben, so bald als möglich vorzustellen.

V

Verantwortliche Stelle
Eine verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet und nutzt oder dies durch andere im Auftrag vornehmen lässt (§ 3 Abs. 7 Bundesdatenschutzgesetz).

W

Widerruf
Betroffene können ihre erteilte Einwilligung widerrufen. Der Widerruf muss höchstpersönlich schriftlich oder in elektronischer Form erklärt werden. Nach herrschender Meinung einer Mindermeinung in der juristischen Literatur sollte auch ein Widerruf durch schlüssiges Verhalten möglich sein. Hierbei ist in Bezug auf Beweisfragen ein nachweisbarer Widerruf vorzuziehen. Der Widerruf muss an denjenigen gerichtet sein, gegenüber welchem ursprünglich die Einwilligung für die Erhebung, Verarbeitung und Speicherung der personenbezogenen Daten erklärt wurde. Durch einen wirksamen Widerruf ist die vorherige Einwilligung mit Wirkung für die Zukunft beseitigt. Dies bedeutet, dass ab dem Zeitpunkt des wirksamen Widerrufs die personenbezogenen Daten des Widerrufenden nicht mehr verwendet werden dürfen.

Herausgeber

Das Handbuch ist im Rahmen des gemeinsamen Projektes „Netzwerk unabhängige Beratung“ des Bundesverband für körper- und mehrfachbehinderte Menschen (bvkm) und des Bundesverband Selbsthilfe Körperbehinderter (BSK) entstanden.

Die teilnehmenden Stellen haben das Datenschutzhandbuch anerkannt und gewährleisten dessen Umsetzung mit Aufnahme der Beratung. Das Handbuch wird stetig fortgeschrieben und geänderten Bedingungen angepasst.

Autorin des Handbuches: **Franziska Facius**,
Leiterin des Netzwerks unabhängige Beratung, BSK (2015–2017)

Unter Mitarbeit von: **Hülya Turhan**,
Leiterin des Netzwerks unabhängige Beratung, bvkm

1. Auflage 2018

Netzwerk unabhängige Beratung

Eine Kooperation von

bvkm. Bundesverband für körper- und mehrfachbehinderte Menschen e.V.

BSK Bundesverband Selbsthilfe Körperbehinderter e.V.

Bundesverband für körper- und
mehrfachbehinderte Menschen e.V.
Brehmstr. 5–7,
40239 Düsseldorf
www.bvkm.de

Bundesverband Selbsthilfe
Körperbehinderter e.V.
Altkrautheimer Str. 20,
74238 Krautheim
www.bsk-ev.org

www.unabhängigeberatung.de