DER PARITÄTISCHE
GESAMTVERBAND

Datenschutz in der Migrationsberatung

Eine Arbeitshilfe für die Migrationsberatung für erwachsene Zuwanderer (MBE)

DEUTSCHER PARITÄTISCHER WOHLFAHRTSVERBAND GESAMTVERBAND e. V. | www.paritaet.org

Publikationen zum Thema Migration
Herausgeber: Der Paritätische Gesamtverband
zu finden auf: **www.migration.paritaet.org**

Case Management in der Migrationsberatung – eine Arbeitshilfe

Berlin 2016

Grundlagen des Asylverfahrens – Eine Arbeitshilfe für Beraterinnen und Berater

4. aktualisierte Auflage
Berlin 2016

Organisation, Reflexion und Qualitätssicherung der Beratungsprozesse. Eine Arbeitshilfe für die Migrationsberatung

Berlin 2016

Ausgeschlossen oder privilegiert? Zur aufenthalts- und sozialrechtlichen Situation von Unionsbürgern und ihren Familienangehörigen

3. aktualisierte Auflage 2017

Wege zeigen – Perspektiven schaffen. Migrationsberatung für erwachsene Zuwanderer (MBE) im Paritätischen – Gelingende Integration vor Ort

Berlin 2010

Soziale Recht für Flüchtlinge

2. Auflage, Dezember 2016, Titel der 1. Aufl. 2012: „Sozialleistungen für Flüchtlinge“

Impressum

Herausgeber:
Der Paritätische Gesamtverband
Oranienburger Straße 13-14
D-10178 Berlin

Telefon: +49 (0) 30/2 46 36-0
Telefax: +49 (0) 30/2 46 36-110

www.paritaet.org
info@paritaet.org

Verantwortlich im Sinne des Presserechts:
Dr. Ulrich Schneider

Autor:
Dr. Thomas Pudelko, Der Paritätische Gesamtverband

Redaktion:
Evîn Kofli, Natalia Bugaj-Wolfram,
Der Paritätische Gesamtverband

Gestaltung:
Christine Maier, Der Paritätische Gesamtverband

Bilder:
© alle Fotolia.com: Destina (Titel, S. 6), momius (S. 4), Alex (S. 8), pathdoc (S. 10), Marco2811 (S. 12), CrazyCloud (S. 17), Zerbor (S. 18)

1. Auflage, November 2017

Gefördert durch:
Bundesministerium des Innern
aufgrund eines Beschlusses des Deutschen Bundestages

MBE
Migrationsberatung für erwachsene Zuwanderer

Inhaltsvezeichnis

Vorwort

Globalisierung und Digitalisierung stellen die Verwendung und Preisgabe persönlicher Daten heute stärker denn je in den Mittelpunkt sozialer Arbeit. Diese Entwicklung lässt sich zum Beispiel über neu entwickelte mobile Technologien festmachen, die unseren Alltag immer mehr bestimmen und Eingang in die Beratungspraxis finden. So wächst durch den Anstieg der Zahlen von Neuzuwanderer/-innen nicht nur die Nachfrage nach Face-to-Face-Beratungen. Oft wird parallel neben der klassischen Form über Emails, Facebook und diversen Apps kommuniziert und beraten, was zwar zum einen den Vorteil hat, dass der Radius an ratsuchenden Personen erweitert wird. Zum anderen steigt jedoch das Risiko, über diese modernen Kanäle sensible Daten unbeabsichtigt preiszugeben.

Über 70 Mitgliedsorganisationen des Paritätischen Wohlfahrtsverbandes setzen das Bundesprogramm der Migrationsberatung für erwachsene Zuwanderer (MBE) tagtäglich und erfolgreich um. Für eine dauerhafte Qualitätssicherung der Arbeit sowohl nach innen als auch nach außen ist es notwendig, insbesondere in sensiblen Arbeitsbereichen wie die des Datenmanagements, sicher handeln zu können.

Ziel dieser Broschüre ist es, den Beratungsfachkräften in den MBE-Einrichtungen Unterstützung zu geben, in datenschutzrechtlichen Zweifelsfällen sicher zu handeln. Vor allem ist Datenschutzmanagement ein Thema, das von der Leitungsebene initiiert und koordiniert wird; dafür soll mithilfe der Broschüre eine Sensibilisierung bei den Berater/-innen stattfinden. Sie soll Hinweise geben, welche Aufgaben hinsichtlich des Datenschutzes die Einrichtungsleitungen haben. Sie soll zudem darin behilflich sein, die Abgrenzung z.B. zwischen Datenschutz, Schweigepflicht, Zeugnisverweigerungsrecht und Offenbarungspflicht klar zu erkennen. Es wird auch auf die Notwendigkeit des technischen Datenschutzes hingewiesen, der jedoch keinen Schwerpunkt in dieser Broschüre einnimmt. Den praxisbezogenen Teil stellt Punkt 5 der Broschüre dar. An der Stelle haben uns MBE-Berater und -beraterinnen Fragen und Erfahrungen aus verschiedenen Situationen der Beratungspraxis zurückgemeldet, die hier gebündelt wiedergegeben werden. Für diese Zuarbeit bedanken wir uns herzlich. Schließlich werden die zentralen Paragrafen der einschlägigen Gesetze und Kommentarstellen im Anhang abgedruckt. Ergänzt wird diese durch eine Sammlung nützlicher Vordrucke und Vorlagen, die im betrieblichen Datenschutz an anderer Stelle so oder ähnlich bereits erfolgreich eingesetzt werden.

Wir bedanken uns herzlich bei Thomas Pudelko, dem Datenschutzbeauftragten des Paritätischen Gesamtverbandes für die Erarbeitung dieser Broschüre sowie den interessanten fachlichen Austausch.

Wir hoffen, dass die Broschüre Sie in Ihrem Beratungsalltag unterstützt!

Evîn Kofli und **Natalia Bugaj-Wolfram**
Referentinnen für Migrationssozialarbeit
Der Paritätische Gesamtverband

1 Datenschutz

Datenschutz umfasst zunächst organisatorische und technische Maßnahmen gegen Missbrauch von Daten innerhalb einer Organisation. In der Debatte um öffentliche Sicherheit geht es dagegen vordringlich um das Abwehren staatlicher Überwachungsinteressen z.B. im Rahmen der Anti-Terror-Maßnahmen.[1] Dies ist nicht Inhalt dieser Veröffentlichung.

Datenschutz im engeren Sinne des Bundesdatenschutzgesetzes (BDSG) bezieht sich vor allem auf personenbezogene Daten: Also alle Informationen, die einen Personenbezug aufweisen. Dies können sein: Adresse, Telefonnummer, Mailadresse, Geburtsdatum, Familienstand, Staatsangehörigkeit, Konfession, Beruf, Foto, Arbeitgeber, Gehalt, Einkommen, Vermögen, Besitz, Urlaubsplanung, Arbeitsverhalten, Arbeitsergebnisse, Zeugnisnoten, Beurteilungen, Krankheiten, Vorstrafen, Steuern, Versicherungen, Vertragskonditionen etc..

Dies bedeutet im Umkehrschluss, dass Datenschutz (im Sinne des BDSG) nur für natürliche Personen gilt. Natürliche Personen werden geboren. Im eingeschränkten Sinne gilt dies auch für juristische Personen, wenn diese auch natürliche Personen sind (z.B. Geschäftsführer, Gesellschafter etc.).

Da jede Organisation mit dieser Art Daten zu tun hat, sollte Datenschutz auch für alle Organisationen ein wichtiges Thema sein.[2]

Darüber hinaus sind einige personenbezogene Daten als besonders schutzwürdig benannt worden (Besondere Daten §3 Abs. 9 BDSG). Dies sind:

- rassische und ethnische Herkunft,
- religiöse oder philosophische Überzeugungen,
- Gewerkschaftszugehörigkeit,
- Gesundheit,
- Sexualleben

Der Umgang mit besonders sensiblen Daten nach §3 Abs. 9 BDSG ist nur erlaubt:

- Wenn es dafür eine vorrangige Rechtsvorschrift[3] gibt.
- Der Betroffene gibt seine Einwilligung (schriftlich)
- Wg. rechtlicher Ansprüche[4]
- Wenn der Betroffene die Daten öffentlich macht
- Für Aufgaben der wissenschaftlichen Forschung / Aufgabenerfüllung im Gesundheitsbereich
- Oder durch erfolgte Vorabkontrolle durch den Datenschutzbeauftragten (DSB)

Ursprünglich wurde unter dem Begriff Datenschutz der Schutz der Daten selbst im Sinne der Datensicherung, z.B. vor Verlust, Veränderung oder Diebstahl verstanden.

Dieses Verständnis fand zum Beispiel seinen Niederschlag im ersten Hessischen Datenschutzgesetz von 1970. Dabei wurde außerdem die schutzrechtliche Aufspaltung von Daten aus der nicht geschützten Sozialsphäre und der geschützten Privat- und Intimsphäre aufgegeben und in einen einheitlichen Schutz von personenbezogenen Daten umgedeutet. In seiner Dissertation „Datenbanken und Persönlichkeitsrecht“ von 1972 hat Seidel das materielle Datenschutzrecht als die Regelung personenbezogener Datenverarbeitungen insgesamt begriffen und gegenüber dem formellen Datenschutzrecht und der Datensicherung abgegrenzt. Mit seiner Arbeit hat er dem Datenschutz die seitdem allgemein und über Deutschland hinaus gebräuchliche Bedeutung gegeben.

1 Hierzu gehören u.a. Staatstrojaner, Videoüberwachung im öffentlichen Raum, automatische Gesichtserkennung inclusive Gemütsinterpretation der erfassten Personen an Gefährdungsbrennpunkten, Funkzellenabfragen etc.

2 Die PQ-Sys des Paritätischen Gesamtverbandes bietet im Rahmen ihrer Seminare und Kurse zum Thema Qualitätsmanagement auch Module zum Thema Datenschutz an.

3 Z.B. ein Gesetz oder eine Durchführungsbestimmung

4 Rentenansprüche, Ansprüche aus Leistungen der Krankenkassen oder der Rehabilitation etc.

Die Europäische Union versteht unter Datenschutz *„insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten" (Art.1 Abs.1 Richtlinie 95/46/EG). Der Europarat definiert Datenschutz als Schutz des „Recht[s] auf einen Persönlichkeitsbereich […] bei der automatischen Verarbeitung personenbezogener Daten"* (Art.1 Europäische Datenschutzkonvention). Im englischen Sprachraum spricht man von privacy (Schutz der Privatsphäre) und von data privacy oder information privacy (Datenschutz im engeren Sinne). Im europäischen Rechtsraum wird in der Gesetzgebung auch der Begriff „data protection" verwendet.

Wer ist verantwortlich?

Laut BDSG (§3, Abs. 7) **ist jede Person, die personenbezogene Daten für sich erhebt oder nutzt, der dies durch andere vornehmen lässt, verantwortlich dafür, dass mit personenbezogenen Daten gemäß der aktuellen Rechtslage umgegangen wird**. Dies bedeutet, dass die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nur mit Einwilligung des Betroffenen[5] geschieht. Diese Einwilligung muss informiert und freiwillig erteilt sein. Sie muss schriftlich, nicht versteckt in den Allgemeinen Geschäftsbedingungen (AGB) und freiwillig erfolgen. Erfolgt die Erhebung im Zusammenhang mit anderen Abfragen, muss diese gesondert hervorgehoben werden.

Die Einwilligung für besondere Daten, also jene über rassische und ethnische Herkunft, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben muss darüber hinaus ausdrücklich erteilt werden. Eine konkludente, „stillschweigende", sich aus dem Verhalten der betroffenen Person schlüssig ableitende Einwilligung ist nicht wirksam. Eine schriftliche Erklärung durch die Personen, deren Daten erhoben werden, ist deshalb in jedem Fall zu empfehlen (Schweigepflichtentbindung).[6]

Schutz personenbezogener Daten vor Missbrauch ist durch

- technische Maßnahmen (Vergabe von Zugriffsrechten, abschließbare Schränke etc.) und
- organisatorische Maßnahmen (ausreichende Informationen der Mitarbeiter/-innen) sicher zu stellen.

Dabei haben folgende Leitmaximen des Datenschutzes zu gelten:

- Nur die Informationen über eine Person sammeln, die für die Durchführung der Arbeit notwendig sind (Erforderlichkeit)
- Informationen nur für den Zweck verwenden, für die sie erhoben wurden (Zweckbindung)
- Die Daten allen Dritten gegenüber verschlossen halten; gegenüber den Betroffenen diese jedoch offenbaren (Transparenz)

5 Betroffener ist derjenige, um dessen Daten es geht.

6 S. dazu das Beispielformular im Anhang (7.7 *Schweigepflichtentbindung*)

Datenerhebung

Personenbezogene Daten sind grundsätzlich beim Betroffenen zu erheben. Die Betroffenen sind dabei über die Rechtsgrundlagen der Erhebung, den Erhebungszweck, den Zweck und die Arte der Verarbeitung unaufgefordert aufzuklären. Daten sollten nur dann gespeichert werden, wenn dies für die konkrete Aufgabenerfüllung aktuell erforderlich ist. Unter Datenspeicherung wird auch das Festhalten von Information in Akten oder anderer schriftlicher Weise verstanden. Daten dürfen nur für den Zweck verwendet werden, für den sie erhoben wurden. Eine Erhebung von Daten für einen späteren Zweck ist unzulässig. Es sei denn der Betroffene stimmt dieser späteren Zweckbindung exklusiv zu. Exklusiv heißt hier: Dieser spätere Zweck muss präzise und für den Betroffenen einsichtig formuliert sein und unabhängig von anderen Zwecken abgefragt werden. Auf welche Art und Weise die Daten erhoben werden (schriftlich, mündlich, online etc.) ist dabei unerheblich.

Datenerhebung für einen späteren Zweck im Kontext der MBE- Beratung tritt auf, wenn Daten zu einem anderen Zweck als nur für die Beratung erhoben werden, z.B. für die Statistik, für die Werbezwecke etc. Das heißt im Umkehrschluss, dass alle Daten, die in einem Erstgespräch aufgenommen werden, um den Fall einordnen und den Handlungsbedarf einschätzen zu können, einem Zweck dienlich sein sollen, nämlich eine sachgerechte Beratung zu ermöglichen.

Datenvermeidung

Um möglichst nur dann Daten zu erheben, wenn dies unumgänglich ist, also sonst das Vorhaben, für das die Daten erhoben werden sollen nicht durchgeführt werden kann, ist bei jeder einzelnen Information zu fragen:

- Ist die Erhebung der Daten notwendig?
- Ist die Erfassung der Daten notwendig?
- Was passiert, wenn nicht?
- Wie lange muss gespeichert werden?
- Ist die Löschung gewährleistet?

Vorabkontrolle

Sollen besonders sensible Daten erhoben, gespeichert, verarbeitet oder übertragen werden, ist eine Vorabkontrolle notwendig, die in der Regel in formalisierter Form durchgeführt wird. Schritte der Vorabkontrolle (s. Anhang, 7.6 *Checkliste zur Vorabkontrolle*) sind:[7]

- Beschreibung des Verfahrens
- Prüfung, ob Einwilligung vorliegt
- Prüfung der Zulässigkeit
- Mitbestimmung?
- Dokumentation

Einwilligung der Betroffenen

Sollen personenbezogene Daten an Dritte übermittelt werden, sind weitere Aspekte zu berücksichtigen. Eine Übermittlung ist immer dann zulässig, wenn der Betroffene eingewilligt hat. Die Einwilligung muss sich auf konkrete Informationen beziehen, kann also nicht pauschal gegeben werden. Formulierung „Hiermit willige ich ein, meine Daten an Dritte zu übermitteln" ist ungültig. (s. Anhang, *7.7 Schweigepflichtentbindung*).

Gesteigerter Schutz

In besonderen Fällen genießen Informationen, die Mitarbeiter/-innen aufgrund einer besonderen persönlichen Vertrauensbeziehung anvertraut wurden, gesteigerten Schutz. Diese Bestimmung (§ 65 SGB VIII) geht allen anderen vor, die sonst eine Weitergabe rechtfertigen würden, auch z.B. der Mitteilungspflicht nach § 138 StGB.

7 Gibt es in der Organisation **keinen** Datenschutzbeauftragten, dann ist die Vorabkontrolle durch die Aufsichtsbehörde, also den Datenschutzbeauftragten (DSB) des jeweiligen Bundeslandes durchzuführen. Der DSB der Organisation soll/muss solche Formulare vorhalten. Das ist keine Aufgaben von Beratungsfachkräften.

1.1 Personenbezogene Daten und deren Gebrauchsgefährdung

Die häufigsten Gebrauchsgefährdungen erfolgen durch Diebstahl, Ausspähen oder unberechtigte Weitergabe.

➲ **Der Diebstahl** von personenbezogenen Daten erfolgt entweder „klassisch" durch Entwenden von Listen oder Datenträgern oder durch digitalen „Einbruch" in IT-Systeme.

➲ **Das Ausspähen** kann durch das Abfotografieren von Listen auf z.B. Anmeldeständen auf Veranstaltungen erfolgen oder auch durch das Installieren von Schadsoftware auf Rechnern, die dann den Rechner nach personenbezogenen Daten durchsuchen oder das Schreiben auf der Tastatur „mitlesen"

➲ **Die unberechtigte Weitergabe** kann in Unwissenheit des Verbotes einer solchen Handlung oder im Wissen darum geschehen. Strafbewehrt ist beides.

Hinzu kommt nicht selten der Verlust personenbezogener Daten durch unachtsamen Umgang. Dies kann durch Vergessen von Unterlagen oder Datenträgern z.B. in Bus/Bahn/Schiff/Flugzeug oder im öffentlichen Raum (Haltestelle, Parkbank, Copyshop, Autodach etc.) geschehen. In allen diesen Fällen müssen die Betroffenen sofort informiert werden (§ 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten, Bundesdatenschutzgesetz (BDSG)). Für diesen Fall sollte jede Organisation, die personenbezogene Daten erhebt, verarbeitet, speichert und/oder weitergibt, einen Notfallplan haben, der mit dem Datenschutzbeauftragten[8] abgesprochen ist.

Bedrohung der Verfügbarkeit

Jede Organisation muss dafür Sorge tragen, dass die Systeme, die mit der Erfassung, Speicherung, Verarbeitung und Weitergabe personenbezogener Daten verwendet werden, angemessenen Schutz gegen Verlust, Funktionsuntüchtigkeit, Ausspähen bieten. Dies geschieht durch Maßnahmen der Datensicherheit, die in weiteren Kapiteln vorgestellt werden.

Bedrohung der Vertraulichkeit

Es ist zu verhindern, dass Unbefugte Daten zur Kenntnis erhalten, oder gar nutzen können, die der datenverarbeitenden Stelle (hier: Beratungsstelle) anvertraut wurden. **Unbefugt sind alle, die nicht von den Dateninhabern berechtigt wurden, deren Daten zu erheben, zu speichern, zu verarbeiten oder zu verändern.** Das können in der Beratungspraxis zum Beispiel die Vorgesetzten, die Kolleg/-innen, Ehrenamtliche, Sprachmittler/-innen und Kooperationspartner/-innen sein. Die Vertraulichkeit ist dann bedroht, wenn Unbefugte Zugriff auf nicht öffentliche personenbezogene Daten erlangen. Dies zu verhindern ist Aufgabe von Sicherheitsmaßnahmen des Datenschutzes.

8 Ausbildung zum Datenschutzbeauftragten ist hier https://akademie.dgi-ag.de/seminare/datenschutz/b?gclid=CjwKEAjwqcHLBRCq5uHTpLL12FISJAD6PgDI2PT4zljO4rFvWrIBuEglZNL9c3uVwVdq_Vxuj52irhoCJMvw_wcB möglich.

2 Gefährdungen

Diese Gefährdungen können durch höhere Gewalt, organisatorische Mängel, menschliches Fehlverhalten und vorsätzliches Handeln geschehen. Unter **höherer Gewalt** sind z.B. Feuer, Blitzschlag, Krieg, Erdbeben oder Überschwemmungen zu verstehen.

➲ **Organisatorische Mängel** sind z.B. nicht vorhandene oder unzureichende Sicherheitskonzepte, veraltete oder unzureichende Hard- und Softwareausstattung, fehlende abschließbare Schränke etc. oder schlecht oder unzureichend geregelte Zuständigkeiten.

➲ Zu **menschlichen Fehlverhalten** sind all die Verhalten zu zählen, die z.B. vorhandene Sicherheitskonzepte ignorieren oder unzureichend umsetzen: Wenn beispielsweise sensible Aufzeichnungen nicht verschlossen aufbewahrt werden, sich über das Passwortmanagement hinweggesetzt wird, Daten entgegen den Sicherheitsrichtlinien auf unsicherem Wege übertragen werden etc.

➲ Eine **vorsätzliche Gefährdung** liegt dann vor, wenn die Personen, die mit personenbezogenen Daten umgehen, diese bewusst und trotz des Wissens, dass sie regelwidrig handeln, anderen offenbaren, weitergeben, für andere Zwecke als vorgeschrieben verwenden oder gar veröffentlichen.

2.1 Maßnahmen gegen Gefährdung

Ein Datenschutzkonzept muss Maßnahmen gegen Gefährdung umfassen, die zweckdienlich und angemessen sind.

An erster Stelle steht die **Personalauswahl**. Mit der Bearbeitung personenbezogener Daten sollen nur solche Personen betraut werden, die absolut vertrauenswürdig sind, die sich der Bedeutung des Datenschutzes bewusst sind, die zuverlässig und sicher in der Handhabung der verwendeten Technik(en) und Verfahren sind. Darüber hinaus ist die regelmäßige Schulung in Fragen des Datenschutzes von sämtlichen Mitarbeiter/-innen angeraten, die in einer Organisation tätig sind, in der personenbezogene Daten erhoben, gespeichert und verarbeitet werden. Hierbei ist neben der Unterweisung der stets aktuellen rechtlichen Situation auch auf die konkrete Arbeitssituation der jeweiligen Organisation einzugehen. Auf jeden Fall sollten die Bedeutung des Verfahrensverzeichnisses (s. Anhang 7.1 *Öffentliches Verfahrensverzeichnis*) und das jeweilige Sicherheitskonzept stets behandelt werden. Dies ist eine Aufgabe der Datenschutzbeauftragten.

> Ein *Verfahrensverzeichnis* ist die schriftliche Aufstellung aller Verfahren in einer Organisation, bei der personenbezogene Daten erhoben, gespeichert, verarbeitet etc. werden. Dieses Verzeichnis ist vom Datenschutzbeauftragten zu führen. Bei der Erstellung mitzuhelfen sind alle Mitarbeiter/-innen einer Organisation verpflichtet.

Regelung der **Zugriffsrechte**: In den meisten Organisationen gibt es bereits Regelungen, wer auf welche Daten Zugriffsrechte besitzt. Allerdings müssen diese auch umgesetzt werden. Als Schwachstelle sei hier die Passwort- und Rechteadministration genannt. Auch dies sollte Thema der regelmäßigen Datenschutzschulungen sein.

Eine Schwachstelle in fast allen Organisationen ist der **Umgang mit Datenträgern**. Durch die Möglichkeit, auf sehr kleinen Datenträgern viele Informationen zu transportieren, wächst die Versuchung, hier unbedarft auch personenbezogene Daten zu transportieren. Doch gerade diese kleinen Datenträger sind anfällig für Verluste. Schnell können sie aus der Tasche fallen. Der Finder kann meist die darauf abgelegten Daten problemlos auslesen und zweckentfremden. Hier sollten grundsätzlich **Verschlüsselungstechniken** eingesetzt werden, die ein missbräuchliches Auslesen dann unmöglich machen. Vor Ort sind diese mobilen Datenträger dann grundsätzlich unter Verschluss aufzubewahren. Ebenfalls grundsätzlich unter Verschluss sind sämtliche Datenträger aufzubewahren, seien dies nun mobile bzw. auswechselbare Laufwerke, CD oder Variochips.[9]

Teil des Datenschutzkonzeptes einer Organisation ist auch die **Regelung des Passworteinsatzes** und deren Verwendung. Für deren Umsetzung sind die IT-Verantwortlichen zuständig. Für die Sensibilisierung für das Thema ist der Datenschutzbeauftragte zuständig.

9 Variochips sind Microbauteile, die z.B. aus einem USB-Chip wahlweise einen Transponder oder einen Microrechner machen können.

Das Datenschutzkonzept einer Organisation muss neben den Regeln für den Umgang mit personenbezogenen Daten auch die **spezifischen Zuständigkeiten** und **Aufbewahrungs- und Löschfristen** regeln (s. 4.1.). Grundsätzlich gilt, dass die oberste Leitung schlussendlich für den Datenschutz die Verantwortung trägt.

3 Datensicherheit

Datensicherheit ist ein häufig mit dem Datenschutz verknüpfter Begriff, der von diesem zu unterscheiden ist: Datensicherheit hat das technische Ziel, Daten jeglicher Art in ausreichendem Maße gegen Verlust, Manipulationen und andere Bedrohungen zu sichern. **Hinreichende Datensicherheit ist eine Voraussetzung für effektiven Datenschutz.** Das BDSG nennt den Begriff der Datensicherheit lediglich in §9a im Zusammenhang mit dem ebenfalls nicht näher definierten „Datenschutzaudit". Unter einem Angriff auf den Datenschutz oder die Datensicherheit (repräsentiert durch zum Beispiel ein Computersystem) versteht man jeden Vorgang, dessen Folge oder Ziel ein Verlust des Datenschutzes oder der Datensicherheit ist. Auch technisches Versagen wird in diesem Sinne als Angriff gewertet.[10]

Der Mangel an Computersicherheit ist eine vielschichtige Bedrohung, die nur durch eine anspruchsvolle Abwehr beantwortet werden kann. Der Kauf und die Installation einer Software ist kein Ersatz für eine umsichtige Analyse der Risiken, möglicher Verluste, der Abwehr und von Sicherheitsbestimmungen.

Technischer Datenschutz – Datensicherheit

Vom organisatorischen Datenschutz unterschieden wird den technischen Datenschutz, auch Datensicherheit genannt. Um einen sicheren Umgang mit personenbezogenen Daten zu gewährleisten ist die Ergänzung des organisationsbezogenen durch den technischen Datenschutz unverzichtbar. Er ist auch durch die EU-Datenschutzgrundverordnung (EU-DSGVO) zwingend vorgeschrieben. Dieser sollte folgende Elemente umfassen:

- IT-Sicherheit,
- Erstellung eines Sicherheitskonzeptes,
- Verabschiedung von Informationsschutz- und Sicherheitsrichtlinien,
- physische, beziehungsweise räumliche Sicherung von Daten,
- Zugriffskontrollen,
- das Aufstellen fehlertoleranter Systeme,
- eingeschränkte Benutzerkonten verwenden,
- restriktive Konfiguration,
- Veraltete, unsichere und unbenutzte Software deinstallieren,
- Sicherungskopien erstellen,
- Antiviren-Software verwenden,
- Firewalls verwenden,
- Sandkästen benutzen,

10 Wird zum Beispiel dem Computer oder Server zu warm, weil die Kühlung es nicht schafft, kann die Funktionsfähigkeit stark beeinträchtigt werden und Daten können verloren gehen.

- aktive Inhalte deaktivieren,
- sensible Daten verschlüsseln sowie sichere Entwicklungssysteme und Laufzeitumgebungen verwenden.

Für einen ersten entsprechenden Check können die entsprechenden Bögen im Anhang (s. Anhang, *7.2 Datenschutz-Checkliste*) verwendet werden. Für die konkrete Überprüfung und technische Anpassung vor Ort sollten ausgewiesene IT-Fachleute herangezogen werden. Weitere Details für den technischen Datenschutz, auch wenn sie Teil des Datenschutzes sind, sind nicht Inhalt dieser Broschüre.

Datenschutz in nicht technischen Systemen

In Abgrenzung zu IT-Sicherheit umfasst Informationssicherheit neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten Informationen, wie zum Beispiel per Hand auf Papier notierte Gesprächsnotizen aus einer Beratungssituation. Auch hier greifen die „Prinzipien der Informationssicherheit", da Vertraulichkeit, Integrität und Verfügbarkeit derartiger Informationen für die Beratungssituation extrem wichtig sind, selbst wenn diese Beratungsstelle vollkommen ohne Einsatz irgendeines IT-Systems betrieben wird.

Die „Prinzipien der Informationssicherheit" sind:

- Datensparsamkeit (nur die Daten sammeln, die für den Zweck notwendig sind),
- Zweckbindung (Daten nur für den Zweck verwenden, für den sie erhoben wurden
- „Weitergabezurückhaltung" (Daten nur dann weitergeben, wenn es gesetzlich geboten oder durch den Dateninhaber freigegeben wurde)
- Transparenz (dem Dateninhaber darlegen, was und warum mit seinen Daten geschieht)

Zum sicheren Umgang mit nichttechnisch gespeicherten personenbezogenen Daten gehören sämtliche Aufzeichnungen, Ausdrucke, Listen, Notizen, Kontaktdaten etc. die einen Bezug zu natürlichen Personen haben. Diese dürfen weder nichtbefugten Personen zugänglich noch bekannt gemacht werden. Dies bedeutet, dass sie weder nicht beaufsichtigt auf Schreibtischen oder sonstigen Ablagen herum liegen dürfen, noch sie unsicher verwahrt werden dürfen. Sämtliche Schriftstücke oder sonstige Materialien (auch solche auf Folien oder anderen Trägermaterialien), auf denen Informationen mit Personenbezug enthalten sind, müssen für unbefugte Dritten unzugänglich aufbewahrt werden, wenn sie nicht im direkten Gebrauch sind.

Beispiel:
Nach einem Beratungsgespräch mit einer ratsuchenden Person müssen die handschriftlichen Notizen, die dabei angefertigt wurden, sicher und unzugänglich für unbefugte Dritte aufbewahrt werden. Ein Verbringen mit anderen Alltagsgegenständen z.B. in einer Tasche, die im weiteren Verlauf des Tages mit sich geführt wird, ist risikobehaftet, da sie verlustig gehen kann.

Werden Handakten oder andere Aufzeichnungen über natürliche Personen geführt, so sind diese bei Nichtbenutzung verschlossen[11] aufzubewahren. Verschlossen bedeutet hier, dass die Akten etc. in einem Schrank oder sonstigen Behälter, der für die Aufbewahrung solcher Dinge geeignet ist, und abschließbar ist, verwahrt werden müssen. Das Schloss ist bei Abwesenheit der befugten Person(en) zu schließen und der Schlüssel vom Schloss abzuziehen. Das Verwahren des Schlüssels ist verbindlich zu regeln. Ein Schlüsselplan ist empfehlenswert.

Gehen solche Materialien verlustig, ist, ähnlich wie bei elektronischen Verlusten, nach einem vorher fest gelegten Notfallplan zu verfahren (s. Anhang, 7.3 *Regelung bei Verletzung der Datensicherheit*)

11 Ein Schlüsselmanagement ist hier zwingend vorgeschrieben.

Sensibilisierung und Befähigung der Mitarbeiter

Ein wichtiger Aspekt in der Umsetzung von Sicherheitsrichtlinien ist die Ansprache der eigenen Mitarbeiter/-innen, die Bildung von sogenannter IT-Security-Awareness. Hier fordern die ersten Arbeitsrichter den Nachweis der erfolgten Mitarbeitersensibilisierung für den Fall eines etwaigen Verstoßes gegen die Firmenrichtlinien. Zusätzliche Bedeutung bekommt diese menschliche Seite der Informationssicherheit außerdem, da Organisationsspionage oder gezielte, wirtschaftlich motivierte Sabotage gegen Unternehmen nicht allein mit technischen Mitteln ausgeführt werden. Um ihren Opfern zu schaden oder Informationen zu stehlen, nutzen die Angreifer beispielsweise Social Engineering (Soziale Manipulation),[12] das nur abzuwehren ist, wenn die Mitarbeiter/-innen über mögliche Tricks der Angreifer informiert sind und gelernt haben, mit potenziellen Angriffen umzugehen. Die Mitarbeitersensibilisierung variiert typischerweise von Organisation zu Organisation, von Präsenzveranstaltungen über webbasierte Seminare bis hin zu Sensibilisierungskampagnen.

Der Fokus verschiebt sich dabei inzwischen von der reinen Sensibilisierung („Awareness“) hin zur Befähigung („Empowerment“) der Anwender, eigenverantwortlich für mehr Sicherheit im Umgang mit IT-gestützten Informationen zu sorgen. In Organisationen kommt dabei dem „Information Security Empowerment“ der Führungskräfte besondere Bedeutung zu, da sie Vorbildfunktion für ihre Abteilungsmitarbeiter/-innen haben und dafür verantwortlich sind, dass die Sicherheitsrichtlinien ihres Verantwortungsbereiches zu den dortigen Arbeitsabläufen passen – eine wichtige Voraussetzung für die Akzeptanz.

12 Mit Social Engineering ist eigentlich „Soziale Manipulation“ gemeint. Dabei wird versucht bei Personen bestimmte Verhaltensweisen oder Reaktionen zu erreichen. In diesem Zusammenhang könnte dies die Preisgabe vertraulicher Informationen sein, um die Person zum Kauf bestimmter Produkte oder zur Freigabe von Geld zu bewegen. Dafür wird das persönliche Umfeld einer Person ausspioniert oder man täuscht eine andere Identität dieser Person gegenüber vor, um weitere Informationen oder Dienstleistungen zu erlangen. Häufig ist auch Ziel das Eindringen in den Rechner des Manipulierten, um dort weiten Schaden anzurichten.

4 Regelungen aus anderen Rechtskreisen

Vom Datenschutz getrennt sind Fragen des Zeugnisverweigerungsrechts, des Auskunftsverweigerungsrechts, die Schweigepflicht, die Verschwiegenheitspflicht und die Offenbarungspflicht. Da diese oftmals nicht auseinander gehalten werden, folgend einige kurze Ausführungen dazu zur Orientierung.

Zeugnisverweigerungsrecht

Das Zeugnisverweigerungsrecht berechtigt den/die Zeugen/Zeugin vor Gericht oder anderen staatlichen Stellen, unter bestimmten Bedingungen die Auskunft in Bezug auf sich oder einen Dritten vollkommen zu verweigern. Davon zu unterscheiden ist das Auskunftsverweigerungsrecht, welches sich lediglich auf bestimmte Fragen bezieht. Weiter ist es vom Aussageverweigerungsrecht, also dem Recht eines Beschuldigten, in Strafverfahren keine Angaben zu dem ihm zur Last gelegten Sachverhalt machen zu müssen, zu unterscheiden.

Es ist u. a. geregelt:

- für den deutschen Zivilprozess in §§383 ff. Zivilprozessordnung (ZPO)
- für den deutschen Strafprozess in §§52 ff. Strafprozessordnung (StPO)

Das hier betrachtete Zeugnisverweigerungsrecht betrifft Aussagen in Vernehmungen gegenüber Ermittlungsbehörden (wie z.B. Staatsanwaltschaft) und Gerichten, darf aber, weil es das restriktivste ist, auch gegenüber allen anderen angewandt werden.

Darüber hinaus darf gegenüber der Polizei immer das Zeugnis verweigert werden, selbst wenn obige Voraussetzungen nicht erfüllt sind. In solchen Fällen kann sich die Polizei aber entschließen, den Fall an die Staatsanwaltschaft abzugeben. Gegenüber der Staatsanwaltschaft darf dann nur noch nach obigem Zeugnisverweigerungsrecht Zeugnis verweigert werden.

Das Zeugnisverweigerungsrecht aus sachlichen Gründen berechtigt nur zur Verweigerung der Antwort auf Einzelfragen. Die deutschen Prozessordnungen räumen sowohl im Zivilprozess als auch im Strafprozess das Recht zur Verweigerung von Aussagen ein, die dem Aussagenden oder einem Angehörigen die Gefahr zuziehen, wegen einer Straftat oder einer Ordnungswidrigkeit verfolgt zu werden (§384 ZPO bzw. §55 StPO). Im Falle von Fragen, deren Beantwortung dem Aussagenden zur Unehre gereichen würde, besteht im Zivilprozess ebenfalls das Recht auf Zeugnisverweigerung. Im Strafprozess hingegen besteht in diesem Fall kein Recht zur Zeugnisverweigerung – es gilt lediglich seit 1994 nach §68a StPO die Vorschrift, dass solche Fragen nur gestellt werden sollen, wenn es unerlässlich ist.

Ein polizeiliches Vernehmungsprotokoll ist im Zivilprozess als Urkundenbeweis verwendbar, selbst wenn der/die Vernommene sein Zeugnisverweigerungsrecht später geltend machen möchte.

Auskunftsverweigerungsrecht

Das Auskunftsverweigerungsrecht ist in § 55 StPO geregelt. Es soll Zeugen oder Angehörige in einem Strafverfahren davor bewahren, Antworten auf bestimmte Fragen zu geben, die sie selbst der Straf- oder Ordnungswidrigkeiten-Verfolgung aussetzen würden. Im Gegensatz zum Zeugnisverweigerungsrecht, das eine komplette Beantwortungsverweigerung beinhaltet, bezieht sich das Auskunftsverweigerungsrecht ausdrücklich nur auf Fragen, deren Beantwortung zur Selbstbelastung eines Zeugen führen könnte.[13]

Schweigepflicht (Verschwiegenheitspflicht)

Die Schweigepflicht gilt gegenüber jedem. Das sind z.B. auch Angehörige eines Betroffenen (auch von Minderjährigen, wobei hier Alter und Einsichtsfähigkeit zu berücksichtigen sind), Berufskollegen und Vorgesetzte des Schweigepflichtigen, soweit diese nicht selbst mit der Bearbeitung des konkreten Falles des Betroffenen befasst sind, die eigenen Freunde und Familienangehörige des Verpflichteten, die Massenmedien und abhängig von gesetzlichen Regelungen: Polizei, Staatsanwaltschaft und Gericht.

13 http://www.juraforum.de/lexikon/auskunftsverweigerungsrecht

Mit der geht in vielen Fällen ein Zeugnisverweigerungsrecht vor Gericht einher, auf das sich die Verpflichteten berufen können (in Deutschland z.B. §53 StPO im Strafverfahren oder §383 ZPO im Zivilverfahren).

Regelungen zur Schweigepflicht gibt es in vielen Gesetzen wie z.B. im ZDVG, PostAGSa, SBG, BVerfGG, StGB. Relevant in diesem Kontext sind jedoch die Regelungen in den Sozialgesetzbüchern und im StGB.

Zur Verschwiegenheit verpflichtet sind gem. §203 StGB (s. Anlage *Gesetzliche Grundlagen*) die in diesem Kontext in Frage kommenden Angehörigen folgender Berufe:

- Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,
- Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer staatlich anerkannten Beratungsstelle,
- Mitglieder oder Beauftragte einer anerkannten Schwangerschaftskonfliktberatungsstelle,
- staatlich anerkannte Sozialarbeiter und Sozialpädagogen,
- der Beauftragte für Datenschutz.

Die Schweigepflicht ist also zum einen an eine ausgeübte Tätigkeit geknüpft und zum anderen gilt sie für bestimmte Berufsgruppen. Für eine MBE-Beratungsstelle bedeutet dies z.B., dass nur die Berater/-innen mit der Qualifikation als staatlich anerkannte/-r Sozialarbeiter/-in und Sozialpädagoge/-in und Berufspsychologen der Schweigepflicht unterworfen sind.

Einige Gesetze des Bundes und der Länder räumen berufsrechtlich bestehenden Verschwiegenheitspflichten, wie sie u. a. für Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung, staatlich anerkannte Sozialarbeiter/-innen und Sozialpädagog/-innen, oder den Beauftragten für Datenschutz bestehen (s. dazu §203 StGB), Vorrang vor den datenschutzrechtlichen Vorschriften ein. Oder anders gesagt, wer die berufsrechtliche Schweigepflicht einhält, beachtet zugleich die Regeln des Datenschutzes. **Wo also der Schutz der besonderen Geheimhaltungspflichten weitergeht als der des BDSG, gilt dieser weitergehende.** Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt[14]. Die Formulierung „bleibt unberührt" verheißt eine parallele Anwendbarkeit zweier Normenkomplexe[15], ohne dass der eine den anderen verdrängt.[16]

14 Bestimmte Berufsgruppen unterliegen Berufsordnungen, die von den jeweiligen Kammervollversammlungen mit Zustimmung der zuständigen Aufsichtsbehörde – den Gesundheitsministerien der Länder – verabschiedet werden. In diesen werden bestimmte Fragen detailliert geregelt. Beispielsweise zu den Themen Ärztliche Schweigepflicht, Datenschutz, Fortbildung, Dokumentationspflicht, Qualitätssicherung, Praxisführung, Berufswidrige Werbung, Kollegialität. An diese haben sich die Gruppenmitglieder- unabhängig von anderen gesetzlichen Regelungen zu halten.

15 Normkomplexe sind hier zum einen Gesetze und zum anderen standesrechtliche Regelungen

16 *Gola* u. a. „BDSG", 7. Aufl. München 2002, § 1 Rdn. 25 (15)

4.1 Weitere rechtliche Fragen

Haftungsfragen

Grundsätzlich gilt, dass die für die Organisation haftenden Personen (Geschäftsführung, Vorstand etc.) auch in datenschutzrechtlichen Aspekten haften. Es sei denn, der/die einzelne Berater/-in handelt vorsätzlich. Um Haftungsfällen vorzubeugen ist zu empfehlen, dass die Organisation ein Datenschutzkonzept, ein IT-Sicherheitskonzept und ein abgestimmtes Verfahren wie im Falle eines Datenschutzschadensfall (mit eindeutigen Zuständigkeiten) zu verfahren ist, entwickelt. Diese zu gestalten und in der Organisation einzuführen, ist Aufgabe der Leitung. Der/Die Datenschutzbeauftrage kann damit beauftragt werden. Hierzu gehören technische und administrative Aspekte wie Zugänge, IT-Schutz, Datensicherung, Aufbewahrungs- und Löschfristen.

Aufbewahrungs-und Löschfristen

Löschfristen sind Gegenstand des Datenschutzes, Aufbewahrungsfristen Gegenstand anderer Rechtskreise. Grundsätzlich müssen personenbezogene Daten gelöscht werden, wenn der Zweck der Datenerhebung erfüllt ist. Sollen Daten über diesen Zeitpunkt hinaus aufbewahrt und genutzt werden, ist dafür entweder bei der Datenerhebung bereits die Erlaubnis einzuholen oder es muss nachträglich dafür das Einverständnis der Dateninhaber eingeholt werden. Auch hier gilt, dass eine generelle Erlaubniseinholung unwirksam ist.

Beschlagnahmeverbot

Das Beschlagnahmeverbot ist in § 97 Abs. 5 StPO geregelt und besagt, dass „Schriftverkehr zwischen dem Beschuldigten und Personen, die ein Zeugnisverweigerungsrecht besitzen" sowie „Aufzeichnungen, die Personen, denen ein Zeugnisverweigerungsrecht zusteht, über ihnen vom Beschuldigten anvertraute Mitteilungen gemacht haben" nicht beschlagnahmt werden dürfen.

Offenbarungspflicht

Offenbarungspflicht heißt, wenn eine Person einer Behörde (z.B. Strafverfolgungsbehörde) gegenüber verpflichtet ist über eine Person und diese betreffende Sachverhalte zu offenbaren, obwohl die zu offenbarende Person dies nicht möchte. Im Allgemeinen besteht keine Offenbarungspflicht, sondern lediglich eine Offenbarungsbefugnis (§ 34 StGB) (s. Anlage Gesetzliche Grundlagen). Allerdings gibt es Ausnahmen. Diese existieren z.B. dann, wenn das Leben oder die Gesundheit akut gefährdet ist und eine Offenbarung (weiteren) Schaden (nach bestmöglicher Einschätzung der Lage) verhindern kann.

Beispiel 1:
Der Sozialarbeiterin einer MBE-Beratungsstelle wird im Rahmen eines Beratungsgesprächs gewahr, dass eine gravierende Vernachlässigung bei einem Kind vorliegen kann. Die Eltern des Kindes sind wegen einer akuten Erkrankung nicht in der Lage, sich um das Kind zu kümmern. Das Jugendamt muss umgehend informiert werden.

Beispiel 2:
Wenn der Berater während der Beratung eines Ratsuchenden Erkenntnisse über eine **zukünftige** Gefährdung anderer Personen erhält, weil der Ratsuchende bspw. einen Mord ankündigt, muss er diese Erkenntnis weitergeben.

Im Gesetz heißt es dazu, wenn *„[…] eine schwerwiegende Straftat geplant wird, die nach §138 StGB anzeigepflichtig ist".* In diesen Fällen besteht eine Offenbarungspflicht (Ausnahmen siehe §139 StGB).

5 Situationen und Fragen aus der Praxis

a) Gibt es eine gesetzliche Grundlage für die Dokumentation der Klientengespräche in der MBE oder müsste man tatsächlich theoretisch von jedem Neuklienten eine Einwilligungserklärung dazu einholen?

Hier ist das Bundesdatenschutzgesetz eindeutig: Da es für diesen Fall keine gesetzliche Extraregelung gibt, muss so wie im BDSG vorgesehen, verfahren werden. Und das besagt, dass von jedem Ratsuchenden eine entsprechende Einwilligungserklärung (Schweigepflichtentbindung) notwendig ist. Die EU-Datenschutzgrundverordnung verschärft diese Regelung noch dahingehend, dass der Ratsuchende auch auf seine Rechte hinsichtlich nachträglicher Löschung seiner Daten hinzuweisen ist.

b) Wann darf man Klientenunterlagen, die für die Beratung relevant waren, vernichten?

Wenn es für Dokumente mit personenbezogenen Inhalten keine gesetzliche Aufbewahrungsfrist gibt, dann sind diese Unterlagen nach Erfüllung des Zwecks, für die sie erhoben wurden, zu löschen bzw. zu vernichten.

c) Wann dürfen elektronische Dokumentations-Klientenakten vernichtet werden?

Wenn keine gesetzliche Aufbewahrungsfrist existiert, sind die elektronischen Akten der Ratsuchenden zu löschen, sobald der Zweck der Ratsuche erfüllt ist und es absehbar ist, dass es zu dem Thema der Ratsuche in näherer Zeit keinen weiteren Beratungsbedarf geben wird.

d) Auf was ist bei der Einbeziehung von Ehrenamtlichen zu achten?

Werden Ehrenamtliche Kräfte in die Arbeit der Beratungsstelle eingebunden, sind diese auf das Datenschutzgesetz und dessen Einhaltung hinzuweisen. Dies ist in schriftlicher Form zu geschehen. Auch für sie gilt die Vertraulichkeit der ihnen anvertrauten Informationen. (s. *Verpflichtungserklärung im Anhang*)

e) Wann sollen Schweigepflichtentbindung und/oder Vollmacht eingeholt werden? Je nach Bedarf?

Neben der Datenschutzerklärung ist es sinnvoll gleichzeitig eine Schweigepflichtentbindung mit dem Erstgespräch einzuholen. Natürlich kann dies auch später erfolgen. Dies ist vom jeweiligen Setting der Beratungsstelle abhängig. Es sollte aber zu Beginn darauf hingewiesen werden, dass diese Schweigepflichtentbindung ggf. später noch erforderlich wird.

f) Akten, also Unterlagen in Papierform werden in einem abgeschlossenen Schrank aufbewahrt. Ist das ausreichend?

Für personenbezogene Daten auf Papier (oder einem anderen Träger mit vergleichbaren Eigenschaften) gilt analog das gleiche, wie für elektronisch/digital gespeicherte personenbezogene Daten. Sie müssen mit vertretbarem Aufwand so geschützt werden, dass damit Unbefugten der Zugriff verwehrt wird und dass sie vor Verlust geschützt sind. Dafür ist die Aufbewahrung in einem abschließbaren Schrank ausreichend, wenn dieser wiederum in einem nicht jedermann zugänglichen Raum, der abschließbar ist, und bei Nichtbenutzung abgeschlossen gehalten wird, steht.

g) Der Laptop mit personenbezogenen Daten ist Passwort geschützt. Ist das ausreichend?

Mobile Rechner wie Laptops, Tablets, Klapprechner, Subnotebook, Netbook, Ultrabook etc. sind, im Gegensatz zu Desktop-Computern, in besonderer Weise Gefahren ausgesetzt. Durch ihre Portabilität können sie leicht verlustig gehen. Damit einhergehend sind dann die darauf befindlichen Daten gefährdet. Mit einem Passwortschutz ist eine einfache Hürde eingebaut. Dieser Passwortschutz sollte allerdings bereits vor dem Start des eigentlichen Betriebssystems (z.B. Windows) installiert sein. Nur so ist gewährleistet, dass nicht unter Umgehung der Sicherungsmodule im Betriebssystem auf die Daten der mobilen Geräte zugegriffen werden kann. Sind auf dem mobilen Gerät besonders sensible Daten gespeichert (rassische und ethnische Herkunft, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörig-

keit, Gesundheit, Sexualleben), sollte ein *Container* installiert werden, der einen besonderen Schutz gewährleistet. Geht das mobile Gerät verloren, kann der nichtberechtigte Nutzer nicht auf die geschützten Daten zugreifen, selbst, wenn der Standardpasswortschutz überwunden wird.

Info:

Ein sicherer Daten-*Container* ist eine mobile Anwendung eines Drittanbieters, mit der ein Bereich des mobilen Endgeräts abgeschottet und abgesichert wird. Das Ziel dieser Container ist es, bestimmte Anwendungen und die damit verbundenen Daten zu isolieren. Damit ergibt sich der Vorteil, dass Malware, System-Ressourcen oder andere Applikationen nicht mit den Daten in diesem sicheren Bereich interagieren können. Somit sind sensible Daten in diesem sicheren Container geschützt.

h) Etliche Empfänger von möglicherweise sensiblen Unterlagen wohnen in einer Sammelunterkunft oder in Wohnanlagen, wo die Briefkastenanlage einen nur unzureichenden Schutz vor Verlust bietet. Wie kann eine sichere Zustellung gewährleistet werden?

Die sichere Zustellung von Unterlagen ist keine Frage des Datenschutzes, sondern des Briefgeheimnisses. Für die sichere Empfangssituation von Post ist der Empfänger bzw. der Betreiber einer Wohnanlage zuständig. Der Absender kann den Empfängern höchstens empfehlen, sich ein Schließfach oder eine Postbox zuzulegen.

i) Unsicherheiten bestehen im Emailverkehr mit Behörden in Bezug auf Datenverschlüsselung. Das geschieht bisher noch nicht, da offensichtlich auch bei Behörden unterschiedliche Verschlüsselungssysteme bestehen! Wie soll man damit umgehen?

Es gibt verschiedene Arten der E-Mail-Verschlüsselung. Das Problem ist, dass der Mailpartner sich jeweils am System des angewendeten Verschlüsselungssystems beteiligen muss. Eine andere Möglichkeit ist, passwortgeschützte Dokumente zu versenden. Dann muss der Empfänger das dazu gehörige Passwort aktiv vom Absender erfragen.

j) Welche Datenschutzprobleme gibt es bei einem serverbasierten Datenbanksystem, zu dem sämtliche Mitarbeiter/-innen einer MBE-Beratungsstelle Zugriff haben?

Dies ist eine anspruchsvolle Aufgabe sowohl für die Zuständigen der IT als auch für die Berater/-innen. Die Berater/-innen müssen bei einem solchen Vorhaben ihre Ansprüche an das Datenbanksystem so formulieren, dass diejenigen, die eine entsprechende Datenbank einrichten, wissen, was gewünscht ist. Unabhängig von den Wünschen der Berater/-innen müssen die Vorgaben des Datenschutzes dabei berücksichtigt werden. Dazu gehört zum einen ein grundsätzlicher Zugriffsschutz, der verhindert, dass Unbefugte keinen Zugriff auf personenbezogene Daten erlangen können. Bei denjenigen, die einen Zugriff berechtigt durchführen sollen, ist die Rechtevergabe[17] genau festzulegen. Und all diese Zugänge sind mit sicheren Passwörtern[18] zu versehen.

k) Viele Ratsuchende möchten, dass man mit ihnen über WhatsApp oder Facebook kommuniziert. Ungeachtet der einfachen Handhabung – ist dies datenschutzrechtlich in Ordnung?

Die Kommunikation mit Ratsuchenden, aber allgemein von dienstlichen Belangen ist über diese Anwendungen hoch problematisch. Zum einen deshalb, weil diese Dienste Adressbücher auf den Kommunikationsgeräten auslesen können und da-

17 Wer darf was lesen, was löschen, was verschieben oder Daten verändern? Welche Daten können/sollen nur von wem gelesen werden können?

18 Ein sicheres Passwort muss mindestens acht Zeichen umfassen. Bereiche mit besonders sensiblen Daten sollten mit einem Passwort von mindestens 20 Zeichen Länge geschützt werden. Das Passwort soll Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern beinhalten. Die Sonderzeichen sind in der Mitte des Passwortes zu platzieren. Das Passwort darf keinen Bezug zu realen Dingen haben (wie z.B. Orte, Geburtsdaten etc.) Muster wie z.B. „123456789" oder „asdfghjkl" sind zu vermeiden. Gute Passwörter ergeben keinen Sinn. So ist „jH_7eefZ5+4Eh" ein gutes Passwort. Jedes Passwort ist nur für eine Anwendung zu verwenden. Das Passwort ist regelmäßig zu ändern (in der Regel alle drei Monate). Das Passwort ist nicht zu notieren und darf an niemanden weitergegeben werden. Eine Ablage z.B. unter der Tastatur oder ähnliche unsichere Orte sind grob fahrlässig.

raus weitere personenbezogene Verknüpfungen herstellen können, zu denen in der Regel die Inhaber dieser Daten keine Erlaubnis erteilt haben. Zum anderen werden für die Kommunikation Daten auf Server im Ausland (i.d.R. in den USA) übertragen. Dies merkt der Anwender nicht. Doch dies ist nach geltendem Datenschutzrecht verboten und müsste vorher auf Sicherheit überprüft und dafür von den Dateninhaber/-innen eine Erlaubnis eingeholt werden.

l) Das Jugendamt vermutet in einer Familie, deren Mutter in der MBE-Beratung als Ratsuchende ist, dass ein Kinderschutzfall besteht (massive Vernachlässigung eines Kindes; ca. 4 Jahre) und bittet die MBE-Beraterin um ihr bekannte Informationen über die Familie. Darf die Beraterin diese Informationen an das Jugendamt weiter geben? Und wenn ja, in welcher Weise?

Da das Jugendamt bereits über eine mögliche Kindesgefährdung informiert ist, muss eine Meldung an das Jugendamt nicht (mehr) erfolgen. Weitere Informationen über die Familie sind nicht weiterzugeben. Egal in welcher Form. Das Jugendamt muss mit den ihm zur Verfügung stehenden Mitteln in diesem Fall tätig werden. Es sei denn, die Ratsuchende stimmt einer Weitergabe solcher Informationen an das Jugendamt schriftlich zu.

m) Im Urlaubsfall, in anderen Vertretungsfällen oder beim Ausscheiden einer Beraterin muss eine Arbeitsübergabe erfolgen. Welche Informationen dürfen hier weitergegeben werden?

Grundsätzlich sind die Mitarbeiter/-innen einer Beratungsstelle zur gegenseitigen Vertretung berechtigt. Dies beinhaltet jedoch z.B. nicht die Weitergabe von Passwörtern für Rechnerzugänge. Hier muss eine IT-Lösung umgesetzt werden, die im Vertretungsfall einen beschränkten Zugriff auf für den Vertretungsfall relevante Daten gewährleistet. Zu überlegen ist, ob sogenannte Teamboxen[19] eingerichtet werden.

Im Beratungsgespräch ist für den Fall einer Arbeitsübergabe eine entsprechende Freigabe durch die Ratsuchenden einzuholen. Bei der Übergabe ist die Vertretung auf besonders schutzwürdige Daten hinzuweisen. Ein Übergabeprotokoll erleichtert ggf. den Nachweis einer korrekten Handhabung. Die Ratsuchende Person kann die – auch interne – Weitergabe besonders schutzwürdiger Informationen ausschließen.

Werden Beratungsfälle in Teambesprechungen, Intervision, Supervision behandelt, sind diese möglichst anonym zu gestalten. Darüber hinaus sind die Beteiligten auf die an diese Konstellationen gebundene berufliche Schweigepflicht hinzuweisen.

n) In der mobilen Beratung werden mobile Rechner verwendet. Was ist bei der Nutzung von öffentlichen WLAN-Verbindungen in Hinsicht auf Datenschutz zu beachten?

Öffentliche WLAN-Verbindungen sind in der Regel völlig ungeschützt. Dies bedeutet, dass unbefugte Dritte recht einfach die Datenkommunikation, die hierüber läuft, mitlesen können. Aus diesem Grund sind hier besondere Vorkehrungen zu treffen. An erster Stelle steht eine verschlüsselte Datenübertragung sowie die Verwendung von sicheren Passwörtern.[20] An zweiter Stelle sollten die Daten auf dem mobilen Rechner besonders gesichert aufbewahrt werden.[21]

19 Unter einer Teambox ist eine Software (meist Cloudbasiert) zu verstehen, die das gemeinsame Arbeiten an Dateien, verbunden mit der Möglichkeit bestimmter Rechtezuweisung (löschen, verschieben, umbenennen etc.) ermöglicht. Beim Zugriff und der Abschottung sind verschiedene Sicherheitsstufen möglich.

20 Esihe Fußnote 18

21 siehe die Kasteninfo zu „Daten-Container“

o) Eine Beraterin wird während eines Beratungsgesprächs nebenbei darüber informiert, dass die Ratsuchende ihre durch das Jobcenter bezahlte Wohnung untervermietet hat, ohne dies weder dem Vermieter noch dem Jobcenter mitzuteilen. Wohnen tut sie in der Sommerwohnung einer Bekannten in einer Gartenanlage. Muss die Beraterin darüber das Jobcenter oder/und den Vermieter informieren?

Die Beraterin muss hier nicht tätig werden. Hier sind keine nicht anders abwendbaren Gefahren für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut in Gefahr. Anders sieht es aus, falls die Beraterin erfährt, das die ratsuchende Person einen Angriffskrieg vorbereitet, Hochverrat oder Landesverrat begehen will, Geld- oder Wertpapierfälschung vorhat, Mord, Totschlag, Völkermord, ein Verbrechen gegen die Menschlichkeit, ein Kriegsverbrechen, Raub oder räuberische Erpressung, oder eine andere schwere Straftat ankündigt, dann muss dieses den Ermittlungsbehörden zur Mitteilung gebracht werden (s. Anhang *§ 138 I StGB*).

p) Es kommt immer wieder vor, dass Behörden (Polizei, Finanzamt, Ausländerbehörde, Jobcenter, BAMF etc.) meist telefonisch, Auskunft über, Ratsuchende oder sogar Gruppen von Ratsuchenden einholen möchten. Wie müssen bzw. sollen sich die Berater/-innen da verhalten?

Hierzu gibt es eine Vielzahl von einzelnen Tatbeständen, die nicht alle einzeln behandelt werden können. Es empfehlt sich aber in jedem Fall um eine schriftliche Anfrage zu bitten und darlegen zu lassen, auf welcher Rechtsgrundlage diese Information weitergegeben werden soll. Wird keine Rechtsgrundlage geliefert, so kann davon ausgegangen werden, dass diese nicht vorhanden ist, und das Auskunftsersuchen sollte zurückgewiesen werden. Es sei denn, der Ratsuchende hat eine Weitergabe dieser Information ausdrücklich und möglichst in Schriftform gestattet.

6 Gesetzliche Grundlagen

- **Art. 1, 2 und 10 des Grundgesetzes**
  Grundlage des heutigen Datenschutzrechtes ist Art. 2 des GG. Danach gehört zum Grundrecht auf freie Entfaltung der Persönlichkeit auch ein Grundrecht auf „informationelle Selbstbestimmung".

  Aufgrund des sog. Volkszählungsurteils vom 15.12.1983 des BVerfG hat der Gesetzgeber das heutige Datenschutzrecht geschaffen.

  „Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art.2 Abs.1 in Verbindung mit Art.1 Abs.1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen." (BVerfGE 65, 1=Dok. E2 zu Art. 2 Abs. 1 GG) In ihm werden grundsätzliche Aspekte des derzeit gültigen Datenschutzes manifestiert. Hierzu gehören u.a.: Zulässigkeit der Verarbeitung, Datensparsamkeit, Zweckbindung (Verbot der Multifunktonalität), Zweckentfremdungsverbot, Transparenzgebot, unabhängige Datenschutzbeauftragte.

- **Bundesdatenschutzgesetz (BDSG)**
- **Telekommunikationsgesetz (TKG)**
  Schutz des Fernmeldegeheimnisses § 88, §§ 91 ff
- **Informations- und Kommunikationsdienstgesetz (IuKDG)**
- **Sozialgesetzbuch (SGB I § 35 Abs.4, SGB VIII §§ 61 Abs.4, 64 Abs.1, 67 Abs.6, 76, 102 Abs.2 Nr. 6, SGB X § 68, 71,85,**
- **Betriebsverfassungsgesetz §§ 75 (2), 80 (1), 87 (1) 6 BetrVG**
- **Strafgesetzbuch StGB § 203**
- **Datenschutzrichtlinie (DSRL) 95/46/EG**
- **Datenschutzgrundordnung (DS-GVO) VO (EU) 2016/679**

Aus den rechtlichen Bestimmungen (Gesetzen und Verordnungen) ergeben sich für die Organisationen (Träger und Einrichtungen) Anforderungen an den Datenschutz.

An erster Stelle ist die Wahrnehmung der Zuständigkeit für den Datenschutz durch die oberste Leitung zu nennen. Je nach Art der Organisation und ihre Ausdifferenzierung sind Vorstand oder Geschäftsführung hier gefragt. Diese können eine Person zum Datenschutzbeauftragten bestellen, die dann im Auftrag der obersten Leitung die Belange des Datenschutzes in einer Organisation wahrnimmt.

Einschlägige Gesetze (Auswahl der im Text erwähnten Paragraphen)

Datenschutzgrundordnung (DS-GVO) VO (EU) 2016/679

Die Datenschutz-Grundverordnung setzt die Richtlinie 95/46/EG außer Kraft. Sie trat am 24. Mai 2016 in Kraft und gilt ab 25. Mai 2018 unmittelbar in allen Staaten der Europäischen Union. Die bisherigen nationalen Regelungen wie das deutsche BDSG werden abgelöst bzw. neu gefasst, um die Regelungsaufträge der Verordnung an den nationalen Gesetzgeber zu erfüllen.

Ab dem 25. Mai 2018 muss der Datenschutzbeauftragte nicht nur auf die Einhaltung der entsprechenden Datenschutzvorschriften hinwirken, sondern erhält nach Art. 39 Abs. 1b) Datenschutz-Grundverordnung (DSGVO) eine umfassende Überwachungspflicht.

Der Schwerpunkt der Tätigkeit des Datenschutzbeauftragten liegt dann nämlich in der: „Überwachung der Einhaltung dieser Verordnung [gemeint ist die DSGVO], anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen."

Zentral ist jedoch die Veränderung von einer Betrachtung der einzelnen Datenverarbeitungsprozesse in einer Organisation hin zu einem geforderten ganzheitlichen Datenschutzmanagement. Damit einher geht auch die Nachweispflicht über die Befolgung aller entsprechenden Grundsätze und Vorschriften in einer Organisation. Hier gehört z.B. auch eine verpflichtende Datenschutzinformation im Internetauftritt. [22] Die Nichtbeachtung dieser Vorschriften aus der DSGVO ist bußgeldbedroht. Besonders die Rechte Betroffener ihre Daten löschen zu lassen ist gestärkt worden. So müssen personenbezogene Daten zukünftig auch dann auf Verlangen gelöscht werden, wenn zuvor eine Einwilligung auf Erhebung, Speicherung etc. gegeben wurde.[23] Es empfiehlt sich deshalb die IT und die Betriebsabläufe dahingehend rechtzeitig zur Inkrafttretung am 25. Mai 2018 zu ertüchtigen. Dies ist originäre Aufgabe des betrieblichen Datenschutzbeauftragten.

Unabhängig von der Anzahl der mit der Datenverarbeitung beschäftigten Personen sieht das BDSG noch eine Reihe weiterer Fälle vor, in denen ein Datenschutzbeauftragter zu bestellen ist. Dies betrifft u.a. Auskunfteien, Adressverlage und Markt- und Meinungsforschungsinstitute sowie Unternehmen, die besonders sensitive Daten verarbeiten (z.B. Gesundheitsdaten).

Bundesdatenschutzgesetz (BDSG)

§ 3 Weitere Begriffsbestimmungen

(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

22 Als Beispiel sei genannt, dass die dienstliche Verwendung von WhatsApp dahingehend bekannt gemacht werden muss, dass z.B. „im Rahmen des Beratungs- und Begleitungsprozesses personenbezogene Daten in die USA übermittelt werden."

23 Es sei denn, andere Rechtsgüter stehen dem entgegen.

§ 4a Einwilligung

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

§ 4d Meldepflicht

(1) Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Maßgabe von § 4e zu melden.

(2) Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.

§ 5 Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Beschreibung der Schutzmaßnahmen erfolgt im Hinblick auf die im BDSG genannten acht Schutzziele. Im Fall einer festgelegten betrieblichen Sicherheitspolitik im Unternehmen erfolgt alternativ der Hinweis auf die Abstimmung mit der Organisationseinheit „IT-Sicherheit".

Die technischen und organisatorischen Maßnahmen zur angemessenen Sicherung der Daten vor Missbrauch und Verlust beinhalten entsprechend dem Bundesdatenschutzgesetz insbesondere:

- **Zutrittskontrolle**, z. B. beim Zutritt zu IT-Räumen wie Serverräumen etc.) Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

- **Zugangskontrolle**, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- **Zugriffskontrolle,** dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- **Weitergabekontrolle**, dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger

nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- **Eingabekontrolle**, dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Durch die **Auftragskontrolle** soll gewährleistet werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur gemäß den Weisungen des Auftraggebers verarbeitet werden können. Rechtlich geregelt und gefordert wird die Auftragskontrolle in den technisch-organisatorischen Maßnahmen des BDSG (Anlage zu § 9 BDSG, Nr. 6). In § 9 Satz 2 BDSG wird präzisiert, dass die Maßnahmen verhältnismäßig sein müssen, also in einem angemessenen Verhältnis zu ihrem jeweils angestrebten Schutzzweck stehen sollten.

- Unter **Verfügbarkeitskontrolle** versteht man, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust zu schützen sind. In der Regel geschieht dies durch fachgerechte regelmäßige Datensicherungen und Backups, aber auch durch einen Notfallplan, Virenschutz und andere Maßnahmen. Gesetzlich geregelt und gefordert wird die Verfügbarkeitskontrolle in den technisch-organisatorischen Maßnahmen des BDSG (Anlage zu § 9 BDSG, Nr. 7). In § 9 Satz 2 BDSG wird präzisiert, dass die Maßnahmen verhältnismäßig sein müssen, also in einem angemessenen Verhältnis zu ihrem jeweils angestrebten Schutzzweck stehen sollten.

- **Trennungskontrolle** besagt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt verarbeitet werden müssen.

§ 34 Auskunft an den Betroffenen

(1) Die verantwortliche Stelle hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

2. den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und

3. den Zweck der Speicherung.

(..)

(1a) Im Fall des § 28 Absatz 3 Satz 4 hat die übermittelnde Stelle die Herkunft der Daten und den Empfänger für die Dauer von zwei Jahren nach der Übermittlung zu speichern und dem Betroffenen auf Verlangen Auskunft über die Herkunft der Daten und den Empfänger zu erteilen. Satz 1 gilt entsprechend für den Empfänger.

§ 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Stellt eine nichtöffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),

2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,

3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder

4. personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und

drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

Strafprozessordnung (StPO)

§ 55 (StPO) Auskunftsverweigerungsrecht

(1) Jeder Zeuge kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihm selbst oder einem der in § 52 Abs. 1 bezeichneten Angehörigen die Gefahr zuziehen würde, wegen einer Straftat oder einer Ordnungswidrigkeit verfolgt zu werden.

(2) Der Zeuge ist über sein Recht zur Verweigerung der Auskunft zu belehren.

§ 64 SGB VIII, Datenübermittlung und -nutzung

(1) Sozialdaten dürfen zu dem Zweck übermittelt oder genutzt werden, zu dem sie erhoben worden sind.

(2) Eine Übermittlung für die Erfüllung von Aufgaben nach § 69 des Zehnten Buches ist abweichend von Absatz 1 nur zulässig, soweit dadurch der Erfolg einer zu gewährenden Leistung nicht in Frage gestellt wird.

(2a) Vor einer Übermittlung an eine Fachkraft, die der verantwortlichen Stelle nicht angehört, sind die Sozialdaten zu anonymisieren oder zu pseudonymisieren, soweit die Aufgabenerfüllung dies zulässt.

(3) Sozialdaten dürfen beim Träger der öffentlichen Jugendhilfe zum Zwecke der Planung im Sinne des § 80 gespeichert oder genutzt werden; sie sind unverzüglich zu anonymisieren.

Sozialgesetzbuch (SGB)

§ 65 SGB VIII, Besonderer Vertrauensschutz in der persönlichen und erzieherischen Hilfe

(1) 1 Sozialdaten, die dem Mitarbeiter eines Trägers der öffentlichen Jugendhilfe zum Zweck persönlicher und erzieherischer Hilfe anvertraut worden sind, dürfen von diesem nur weitergegeben werden

1. mit der Einwilligung dessen, der die Daten anvertraut hat, oder

2. dem Familiengericht zur Erfüllung der Aufgaben nach § 8a Absatz 2, wenn angesichts einer Gefährdung des Wohls eines Kindes oder eines Jugendlichen ohne diese Mitteilung eine für die Gewährung von Leistungen notwendige gerichtliche Entscheidung nicht ermöglicht werden könnte, oder

3. dem Mitarbeiter, der aufgrund eines Wechsels der Fallzuständigkeit im Jugendamt oder eines Wechsels der örtlichen Zuständigkeit für die Gewährung oder Erbringung der Leistung verantwortlich ist, wenn Anhaltspunkte für eine Gefährdung des Kindeswohls gegeben sind und die Daten für eine Abschätzung des Gefährdungsrisikos notwendig sind, oder

4. an die Fachkräfte, die zum Zwecke der Abschätzung des Gefährdungsrisikos nach § 8a hinzugezogen werden; § 64 Abs. 2a bleibt unberührt, oder

5. unter den Voraussetzungen, unter denen eine der in § 203 Abs. 1 oder 3 des Strafgesetzbuches genannten Personen dazu befugt wäre.

2 Gibt der Mitarbeiter anvertraute Sozialdaten weiter, so dürfen sie vom Empfänger nur zu dem Zweck weitergegeben werden, zu dem er diese befugt erhalten hat.

(2) § 35 Abs. 3 des Ersten Buches gilt auch, soweit ein behördeninternes Weitergabeverbot nach Absatz 1 besteht.

Strafgesetzbuch (StGB)

§ 138 StGB

(1) Wer von dem Vorhaben oder der Ausführung

1. einer Vorbereitung eines Angriffskrieges (§ 80),

2. eines Hochverrats in den Fällen der §§ 81 bis 83 Abs. 1,

3. eines Landesverrats oder einer Gefährdung der äußeren Sicherheit in den Fällen der §§ 94 bis 96, 97a oder 100,

4. einer Geld- oder Wertpapierfälschung in den Fällen der §§ 146, 151, 152 oder einer Fälschung von Zahlungskarten mit Garantiefunktion und Vordrucken für Euroschecks in den Fällen des § 152b Abs. 1 bis 3,

5. eines Mordes (§ 211) oder Totschlags (§ 212) oder eines Völkermordes (§ 6 des Völkerstrafgesetzbuches) oder eines Verbrechens gegen die Menschlichkeit (§ 7 des Völkerstrafgesetzbuches) oder eines Kriegsverbrechens (§§ 8, 9, 10, 11 oder 12 des Völkerstrafgesetzbuches),

6. einer Straftat gegen die persönliche Freiheit in den Fällen des § 232 Abs. 3, 4 oder Abs. 5, des § 233 Abs. 3, jeweils soweit es sich um Verbrechen handelt, der §§ 234, 234a, 239a oder 239b,

7. eines Raubes oder einer räuberischen Erpressung (§§ 249 bis 251 oder 255) oder

8. einer gemeingefährlichen Straftat in den Fällen der §§ 306 bis 306c oder 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 4, des § 309 Abs. 1 bis 5, der §§ 310, 313, 314 oder 315 Abs. 3, des § 315b Abs. 3 oder der §§ 316a oder 316c zu einer Zeit, zu der die Ausführung oder der Erfolg noch abgewendet werden kann, glaubhaft erfährt und es unterläßt, der Behörde oder dem Bedrohten rechtzeitig Anzeige zu machen, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer

1. von der Ausführung einer Straftat nach § 89a oder

2. von dem Vorhaben oder der Ausführung einer Straftat nach § 129a, auch in Verbindung mit § 129b Abs. 1 Satz 1 und 2, zu einer Zeit, zu der die Ausführung noch abgewendet werden kann, glaubhaft erfährt und es unterlässt, der Behörde unverzüglich Anzeige zu erstatten. § 129b Abs. 1 Satz 3 bis 5 gilt im Fall der Nummer 2 entsprechend.

(3) Wer die Anzeige leichtfertig unterläßt, obwohl er von dem Vorhaben oder der Ausführung der rechtswidrigen Tat glaubhaft erfahren hat, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

§ 34 Rechtfertigender Notstand

Wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, handelt nicht rechtswidrig, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Dies gilt jedoch nur, soweit die Tat ein angemessenes Mittel ist, die Gefahr abzuwenden.

§ 203 Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung,

3. Rechtsanwalt, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,

4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,

4a. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,[24]

5. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder

6. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

24 Die anerkannten Beratungsstellen nach § 218b Abs. 2 Nr. 1 StGB stehen den anerkannten Beratungsstellen nach § 3 des G über die Aufklärung, Verhütung, Familienplanung und Beratung gleich gem. BVerfGE v. 4.8.1992 I 1585 - 2 BvO 16/92 u. a. -

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger,

2. für den öffentlichen Dienst besonders Verpflichteten,

3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,

4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,

5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder

6. die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist,

anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.

(2a) Die Absätze 1 und 2 gelten entsprechend, wenn ein Beauftragter für den Datenschutz unbefugt ein fremdes Geheimnis im Sinne dieser Vorschriften offenbart, das einem in den Absätzen 1 und 2 Genannten in dessen beruflicher Eigenschaft anvertraut worden oder sonst bekannt geworden ist und von dem er bei der Erfüllung seiner Aufgaben als Beauftragter für den Datenschutz Kenntnis erlangt hat.

(3) Einem in Absatz 1 Nr. 3 genannten Rechtsanwalt stehen andere Mitglieder einer Rechtsanwaltskammer gleich. Den in Absatz 1 und Satz 1 Genannten stehen ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. Den in Absatz 1 und den in Satz 1 und 2 Genannten steht nach dem Tod des zur Wahrung des Geheimnisses Verpflichteten ferner gleich, wer das Geheimnis von dem Verstorbenen oder aus dessen Nachlaß erlangt hat.

(4) Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(5) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

7 Anhang

7.1 Öffentliches Verfahrensverzeichnis (für jeden einsehbar oder anforderbar)

Namen der Organisation etc. ……

……

Leitung
Verantwortlich für die EDV/IT……

Anschrift ……

Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung.
Beschreibung der betroffenen Personengruppen

Beschreibung der Datenkategorien
Die Datenerhebung, -verarbeitung und -nutzung erfolgt zur Ausübung der oben genannten Zwecke (Punkt 5).
- ……..
- Daten von Lieferanten (z.B. Büromaterial)
- Daten von Dienstleistern (Steuerberatung, RA,
- Daten zur Erfüllung sozialversicherungsrechtlicher und sonstiger gesetzlicher Verfahren

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden.
Intern:
- Mitarbeiter/-innen,
- Vorstand,
- ……..

Extern:
- Krankenkassen
- Ärzte
- Kreditinstitute
- Steuerberater
- öffentliche Stellen, die Daten aufgrund gesetzlicher Vorschriften erhalten, wie z.B. Finanzbehörden, Sozialversicherungsträger
- externe Auftragnehmer entsprechend §11 BDSG

Regelfristen für die Löschung der Daten
Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und -fristen erlassen. Nach Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig gelöscht, wenn sie nicht mehr zur Vertragserfüllung erforderlich sind, soweit gesetzlich Aufbewahrungspflichten und -fristen dem nicht entgegenstehen. Sofern Daten hiervon nicht berührt sind, werden sie gelöscht, wenn die unter 5. genannten Zwecke wegfallen.

Geplante Datenübermittlung an Drittstaaten
Eine Übermittlung von Daten in Drittstaaten ist nicht vorgesehen.

Datenschutzbeauftragter
N.N.
E-Mail:

7.2 Datenschutz-Checkliste für Organisationen

Bestellung eines Datenschutzbeauftragten

Gesetzlich erforderlich?

☐ Ja ☐ Nein

Ist ein Datenschutzbeauftragter bestellt?

☐ Ja ☐ Nein

Ist die erforderliche Fachkunde des Datenschutzbeauftragten nachgewiesen?

☐ Ja ☐ Nein

Ist die „Zuverlässigkeit" des Datenschutzbeauftragten gewährleistet („keine Interessenskonflikte")?

☐ Ja ☐ Nein

Ist der Datenschutzbeauftragte direkt der Geschäftsleitung unterstellt und in die Informationsprozesse im Unternehmen, insbesondere bei der Planung und Anschaffung von Informationstechnologie eingebunden?

☐ Ja ☐ Nein

Hat der Datenschutzbeauftragte die Möglichkeit, sich regelmäßig fortzubilden (Schulung, Literatur etc.)

☐ Ja ☐ Nein

Verpflichtung auf das Datengeheimnis

Sind alle Beschäftigten auf das Datengeheimnis i.S.d. § 5 BDSG verpflichtet worden?

☐ Ja ☐ Nein

Werden auch externe Mitarbeiter (z.B. Reinigungskräfte, Werkstudenten u.ä.) auf das Datengeheimnis verpflichtet?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Verfahrensverzeichnis / Verarbeitungsübersicht

Gibt es ein Verfahrensverzeichnis (für jeden einsehbar und anforderbar)

☐ Ja ☐ Nein

Gibt es eine interne Übersicht der Verfahren, mit denen personenbezogene Daten verarbeitet werden („internes Verfahrensverzeichnis" / Verarbeitungsübersicht)

☐ Ja ☐ Nein

Ist gewährleistet, dass bei der Anschaffung/Änderung neuer IT, bei der Gestaltung neuer IT-Abläufe oder der Änderung im IT-Bereich eine Anpassung der Verarbeitungsübersicht erfolgt?

☐ Ja ☐ Nein

Meldepflicht

„Gegenausnahmen" vorhanden (geschäftsmäßige Übermittlung von Daten oder für Zwecke der Markt- und Meinungsforschung)?

☐ Ja ☐ Nein

Falls ja, wurde Meldepflicht eingehalten?

☐ Ja ☐ Nein

Vorabkontrolle

Werden Vorabkontrollen (§ 4d Abs. 5, 6 BDSG) vor der Einführung von automatisierten Datenverarbeitungsvorgängen durchgeführt, wenn diese Vorgänge besondere Risiken für die Rechte der Betroffenen beinhalten?

☐ Ja ☐ Nein

IT-Sicherheit

Technische und organisatorische Maßnahmen gemäß § 9 BDSG und der Anlage zu § 9 Satz 1 BDSG
Gibt es schriftliche Dokumentation der technischen und organisatorischen Maßnahmen i.S.d. § 9 BDSG

☐ Ja ☐ Nein

Gibt es eine Leitlinie zur Informationssicherheit?

☐ Ja ☐ Nein

Gibt es eine IT-Richtlinie (o.ä.) für Beschäftigte, aus der sich ergibt, ob und wie diese IT-Systeme im Unternehmen verwenden dürfen?

☐ Ja ☐ Nein

Gibt es eine Risiko- und Schwachstellenanalyse im Hinblick auf Räume, IT-Systeme, IT-Applikationen und Netzwerkkomponenten?

☐ Ja ☐ Nein

Gibt es einen Notfallplan?

☐ Ja ☐ Nein

Compliance bei der Verarbeitung von Daten

Direkterhebung
Werden personenbezogene Daten grundsätzlich selbst beim Betroffenen erhoben?

☐ Ja ☐ Nein

Rechtsgrundlage

Wird Sorge dafür getragen, dass personenbezogene Daten grundsätzlich nur dann verarbeitet werden, wenn dies zur Erbringung vertraglicher Leistungen erforderlich, im Rahmen einer Interessenabwägung zulässig ist oder eine Einwilligung des Betroffenen vorliegt?

☐ Ja ☐ Nein

Einwilligung

Wird bei der Verwendung von Einwilligungen darauf geachtet, dass der Betroffene über Zweck, Art und Umfang der Verwendung der von ihm freiwillig angegebenen Daten informiert wird?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Kann der Betroffene die Einwilligungserklärung auch ohne Fachkenntnisse verstehen und erkennen, dass die Einwilligung freiwillig ist und ggf. welche Konsequenzen eine Nichterteilung einer Einwilligung hat?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Ist im Falle eines Widerrufs der Einwilligung gewährleistet, dass die betroffenen personenbezogenen Daten nicht weiter verwendet werden?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Auftragsdatenverarbeitung

Gibt es eine Übersicht aller Dienstleister/Lieferanten, die entweder Daten im Auftrag des Unternehmens verarbeiten oder IT-Systeme warten und pflegen?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Wird Sorge dafür getragen, dass bei den Auftragnehmern/Dienstleistern ein Auftragsdatenverarbeitungsvertrag nach den Vorgaben des § 11 BDSG geschlossen wurde (und wird)?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Gibt es ein Muster für einen Auftragsdatenverarbeitungsvertrag im Unternehmen?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Wird Sorge dafür getragen, dass der Auftragnehmer bei einer Auftragsdatenverarbeitung vor Vertragsschluss im Hinblick auf die getroffenen IT-Sicherheitsmaßnahmen kontrolliert wird?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Ist gewährleistet, dass Auftragnehmer regelmäßig (grundsätzlich 1x jährlich) im Hinblick auf Änderungen im Bereich der IT-Sicherheit kontrolliert werden?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Informationspflicht bei „Datenpannen“

Werden Verfahren, mit denen besondere Arten personenbezogener Daten (§ 3 Absatz 9), personenbezogene Daten, die einem Berufsgeheimnis unterliegen, personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder personenbezogene Daten zu Bank- oder Kreditkartenkonten gesondert intern gekennzeichnet bzw. überwacht?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Wird Sorge dafür getragen, dass im Falle einer unbefugten Kenntnisnahme durch Dritte von Daten, die nach § 42a BDSG geschützt sind, sofort der Datenschutzbeauftragte informiert wird?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Gibt es einen Ablaufplan für den Fall einer Datenpanne?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Betroffenenrechte

Gibt es ein „Betroffenenmanagement“ dahingehend, dass Betroffene, die ihre Betroffenenrechte i.S.d. BDSG geltend machen, direkten Kontakt zum Datenschutzbeauftragten erhalten?

☐ Ja ☐ Nein

Werden Auskunftsersuchen von Betroffenen kurzfristig und vollständig beantwortet?

☐ Ja ☐ Nein

Gibt es ein Löschkonzept im Unternehmen, das Regelfristen für die Löschung von Daten vorsieht?

☐ Ja ☐ Nein

Internet / E-Mail

Gibt es für die Internetseite des Unternehmens gesonderte Datenschutzhinweise, die von jeder Seite der Internetseite aus erreichbar sind (nicht nur im „Impressum“)

☐ Ja ☐ Nein

Wird über Webanalyse-Software informiert?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Wird über die Verwendung und das „Blocken“ von Cookies informiert?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Wird über Tracking-Pixel oder sonstige verwendete Methoden für Zwecke der Werbung oder des Marketings informiert und werden Möglichkeiten für ein „Opt-Out“ angezeigt?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

E-Mail-Marketing

Wird ein E-Mail-Newsletter angeboten?

☐ Ja ☐ Nein

Werden Newsletter-Abonnenten hinreichend über Zweck, Art und Umfang der Datenverarbeitung beim E-Mail-Newsletter informiert (insbes. Tracking von „Open Rates“, „Click Rates“ u.Ä.)?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Gibt es ausreichende vertragliche Regelungen zur Verwendung der Daten durch einen externen Newsletter-Dienstleister (z.B. Auftragsdatenverarbeitungsvertrag, Einwilligung etc.)

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Private Internet-/E-Mail-Nutzung im Unternehmen

Gibt es eine unternehmensinterne Regelung zur privaten Nutzung des Internets im Unternehmen

☐ Ja ☐ Nein

Gibt es eine unternehmensinterne Regelung zur privaten Nutzung von E-Mail im Unternehmen

☐ Ja ☐ Nein

Betriebsrat

Gibt es einen Betriebsrat im Unternehmen

☐ Ja ☐ Nein

Gibt eine Übersicht der Betriebsvereinbarungen, die Regelungen zum Umgang mit personenbezogenen Daten enthalten?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Datenflüsse im Konzern

Gehören mehrere Unternehmen zur Unternehmensgruppe („Konzern")?

☐ Ja ☐ Nein

Falls ja, gibt es Regelungen zur gemeinsamen Nutzung von Daten oder IT-Infrastrukturen im Unternehmen?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Grenzüberschreitender Datenverkehr
Werden Daten des Unternehmens im Ausland verarbeitet bzw. in das Ausland übermittelt?

☐ Ja ☐ Nein

Europäische Union / EWR

Ist im Falle einer Verarbeitung von Daten in anderen EU-Mitgliedsstaaten oder EWR-Staaten gewährleistet, dass eine Rechtsgrundlage für die Verwendung im Ausland besteht (z.B. § 28 BDSG und ggf. Auftragsdatenverarbeitung)?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

„Drittstaaten"

Werden Daten in „Drittstaaten" verwendet bzw. dorthin übermittelt?

☐ Ja ☐ Nein

Ist vom Unternehmen geprüft worden, ob es für die Übermittlung in den Drittstaat bzw. die Verarbeitung dort eine Rechtsgrundlage im BDSG gibt („erste Stufe")?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Handelt es sich bei dem Drittstaat um einen Staat mit „angemessenen Datenschutzniveau"?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Gibt es eine Einwilligung des Betroffenen zur Übermittlung von personenbezogenen Daten an das Unternehmen in dem Drittstaat?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Ist mit dem Unternehmen in dem Drittstaat ein Vertrag auf Basis der EU-Standardvertragsklauseln geschlossen worden?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Befindet sich das Unternehmen, zu dem Daten übermittelt werden, in den USA und befindet sich dieses in der „Safe Harbor"-Liste?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Wurde die Einhaltung der Safe-Harbor-Prinzipien durch das Unternehmen in dem Drittstaat von Ihrer Organisation geprüft?

☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Stand: 08.07.2015

7.3 Regelung bei Verletzung der Datensicherheit

Zweck und Ziel

Diese Verfahrensanweisung beschreibt den Umgang mit Situationen, in denen Datensicherheitsrichtlinien (Sicherheitspolitik) verletzt wurden.

Zweck dieser Verfahrensanweisung ist der Schutz der Betroffenen vor der Gefahr, welche die Datenverarbeitung für die Dateninhaber mit sich bringt. Geschützt werden alle „natürliche Personen" vor der Verletzung ihres Persönlichkeitsrechts von denen dem *(Name der Organisation)* die Daten überlassen wurden.

Datenschutz ist hier die Beachtung der rechtlichen, administrativen und technischen Vorgaben für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten.

Eine Verletzung von Datensicherheitsrichtlinien liegt auf jeden Fall vor, wenn:

a) Die Integrität von Datensätzen personenbezogener Daten verletzt ist (sie z.B. nicht mehr lesbar sind oder nicht mehr bearbeitet werden können),

b) Datensätze personenbezogener Daten verloren gegangen sind bzw. deren Verbleib unklar ist,

c) Datensätze personenbezogener Daten in den Besitz Dritter Unbefugter gelangt sind,

d) Datensätze personenbezogener Daten unbeabsichtigt gelöscht worden sind,

e) Datensätze personenbezogener Daten beabsichtigt gelöscht wurden, aber deren Löschung nicht vorgesehen war.

Geltungsbereich

Diese Verfahrensanweisung richtet sich an alle Teilbereiche des (Organisation bzw. Träger) sowie alle unselbständigen und selbständigen Untereinheiten.

Begriffe, Definitionen

Der Datenschutz, um den es hier geht, bezieht sich ausschließlich auf Daten natürlicher Personen, also aller geborenen Menschen, die datenmäßig beim *(Name der Organisation)* in Erscheinung treten. Das sind alle Mitarbeiter/-innen, aber auch Auszubildende, Besucher/-innen, Praktikant/-innen und Teilnehmer/-innen von Veranstaltungen in der Zuständigkeit des *(Name der Organisation)*

Unter personenbezogenen Daten sind alle Einzelangaben über persönliche oder sächliche Verhältnisse gemeint, die einer natürlichen Person zugeordnet werden können. Dies sind z.B.: Adresse, Telefonnummer, persönliche Mailadresse, Geburtsdatum, Familienstand, Staatsangehörigkeit, Konfession, Beruf, Foto, Video, Arbeitgeber, Gehalt, Einkommen, Vermögen, Besitz, Urlaubsplanung, Arbeitsverhalten, Arbeitsergebnisse, Zeugnisnoten, Beurteilungen, Krankheiten, Vorstrafen, Steuern, Versicherungen, Vertragskonditionen etc.

Verfahren

Wird festgestellt, dass

- besondere Arten personenbezogener Daten (Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben),
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen,

oder

- personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, muss *(Name der Organisation)* dies unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der vom *(Name der Organisation)* daraufhin ergriffenen Maßnahmen enthalten. (§ 42a BDSG)

Verfahren

Diejenige Person, die feststellt, dass eine relevante Verletzung der Sicherheitspolitik erfolgt ist, hat diesen Sachstand unverzüglich der im *(Name der Organisation)* zuständigen Leitungsperson sowie dem Datenschutzbeauftragten (DSB) mitzuteilen.

Zu a): Es muss überprüft werden, ob die Unlesbarkeit/Unbearbeitbarkeit der Daten durch einen Softwarefehler der Anwendungssoftware,

- durch einen Bedienungsfehler,
- durch Schadsoftware,
- durch externe Softwaremanipulation,

oder

- durch mechanische Einflüsse hervorgerufen wurde.

Eine Wiederherstellung / Reproduktion der unbrauchbar gewordenen Datensätze ist einzuleiten, wenn dies unter vertretbarem Aufwand möglich ist.

Nach der Ursachenanalyse sind Maßnahmen zur Vermeidung einer Wiederholung einzuleiten.

Zu b): Es muss überprüft werden, ob die Daten mit ausschließender Wahrscheinlichkeit nicht unbefugten Dritten anheimgefallen sind. Ist dies nicht auszuschließen, ist wie unter 1.3 zu verfahren.

Eine Wiederherstellung / Reproduktion der verlustig gegangenen Datensätze ist einzuleiten, wenn dies unter vertretbarem Aufwand möglich ist.

Nach der Ursachenanalyse für den Verlust sind Maßnahmen zur Vermeidung einer Wiederholung einzuleiten.

Zu c): Besteht der begründete Verdacht, dass personenbezogene Daten in den Besitz unbefugter Dritter gelangt sind, sind Unverzüglich in jedem Fall geeignete Maßnahmen zur Sicherung der Daten zu ergreifen. Die Aufsichtsbehörde sowie die betroffenen Personen sind sodann unverzüglich zu informieren. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten.

Der Ablauf des Datenverlustes ist zu rekonstruieren.

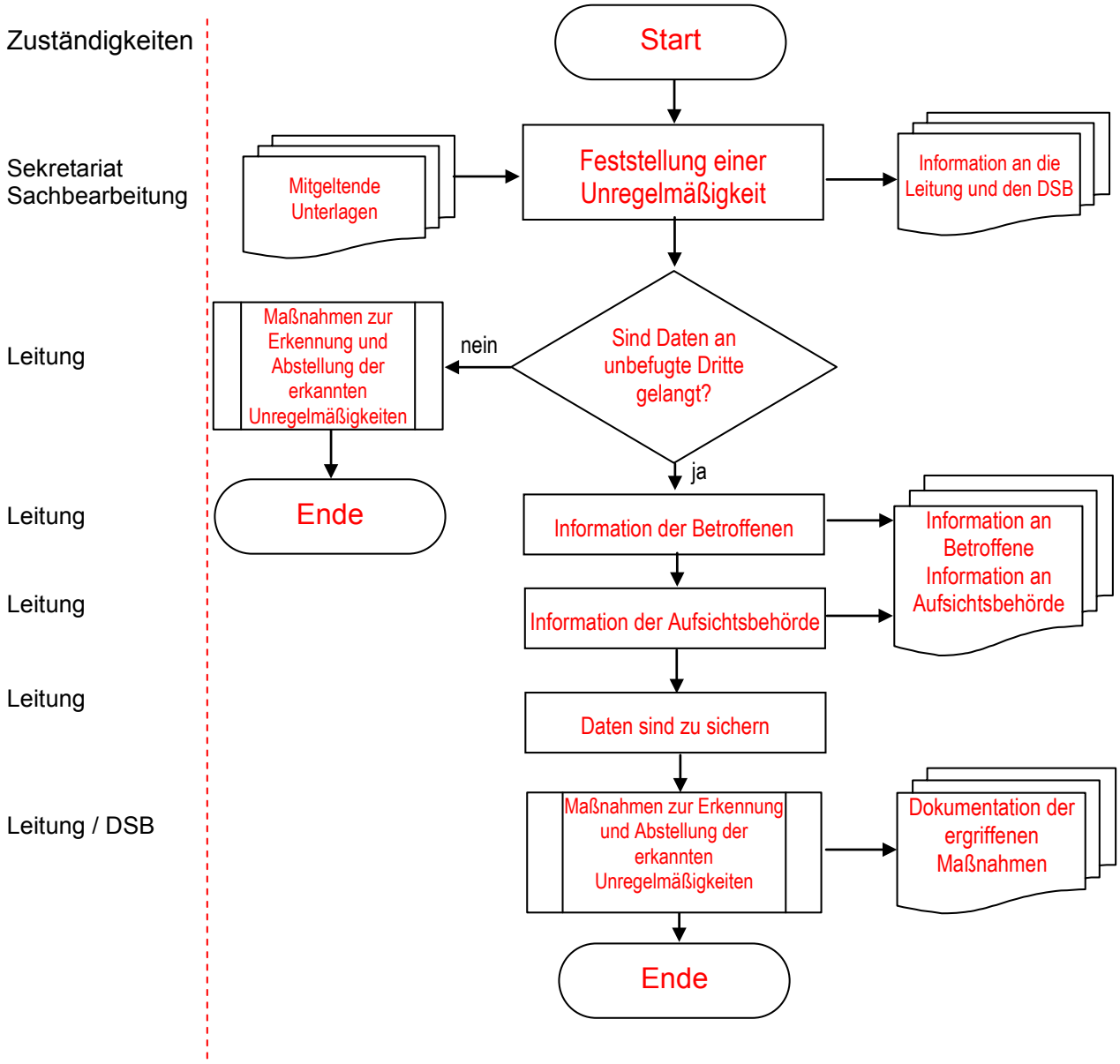
Die Ergebnisse sind zu dokumentieren.

Diese Dokumentation muss folgende Elemente mindestens umfassen:

- Fehlerbewertung,
- Ermittlung der Ursachen der Fehler,
- Beurteilung des Handlungsbedarfs, um das erneute Auftreten des Fehlers zu verhindern,
- Ermittlung und Verwirklichung der erforderlichen Maßnahmen,
- Aufzeichnung der Ergebnisse der ergriffenen Maßnahmen,
- Bewertung der ergriffenen Korrekturmaßnahmen.

Es ist festzuhalten, wer was wann dokumentiert hat. Ist der Fehler durch organisatorische Unzulänglichkeiten entstanden, sind diese abzustellen.

Ablaufdiagramm zu c)



Zu d): Sind Datensätze personenbezogener Daten unbeabsichtigt gelöscht worden, ist zu überprüfen, ob die Datensätze an anderer Stelle in aktueller oder zeitnah erstellter Vorläuferversion vorhanden sind (Backupversion). Ist dies der Fall, so sind die Datensätze im Rückspeicherverfahren wieder auf den aktuellsten Stand zu bringen; ggf. müssen verloren gegangene Daten neu bzw. nacherhoben werden. Existiert keine Sicherungskopie, so ist zu überprüfen, mit welchem Aufwand die Daten rekonstruiert werden können. Für diesen Fall ist eine sofortige Arbeitseinstellung am entsprechenden Gerät vorzunehmen. Unverzüglich sind die zuständige Leitungskraft, der IT-Zuständige sowie der DSB zu informieren.

Der Ablauf des Datenverlustes ist zu rekonstruieren.

Die Ergebnisse sind zu dokumentieren.

Diese Dokumentation muss folgende Elemente mindestens umfassen:

- Fehlerbewertung,
- Ermittlung der Ursachen der Fehler,
- Beurteilung des Handlungsbedarfs, um das erneute Auftreten des Fehlers zu verhindern,
- Ermittlung und Verwirklichung der erforderlichen Maßnahmen,
- Aufzeichnung der Ergebnisse der ergriffenen Maßnahmen,
- Bewertung der ergriffenen Korrekturmaßnahmen.

Es ist festzuhalten, wer was wann dokumentiert hat.

Ist der Fehler durch organisatorische Unzulänglichkeiten entstanden, sind diese abzustellen.

Zu e): Sind Datensätze personenbezogener Daten beabsichtigt gelöscht wurden, obwohl deren Löschung nicht vorgesehen war, ist zu überprüfen, ob die Datensätze an anderer Stelle in aktueller oder zeitnah erstellter Vorläuferversion vorhanden sind (Backupversion). Ist dies der Fall, so sind die Datensätze im Rückspeicherverfahren wieder auf den aktuellsten Stand zu bringen; ggf. müssen verloren gegangene Daten neu bzw. nacherhoben werden. Existiert keine Sicherungskopie, so ist zu überprüfen, mit welchem Aufwand die Daten rekonstruiert werden können. Für diesen Fall ist eine sofortige Arbeitseinstellung am entsprechenden Gerät vorzunehmen. Unverzüglich sind die zuständige Leitungskraft, der IT-Zuständige sowie der DSB zu informieren.

Weiter ist wie bei d) zu verfahren.

Vorbeugungsmaßnahmen gegen Datenverlust bzw. Datenmissbrauch

Die [*Name der Organisation*] muss Maßnahmen zur Beseitigung möglicher Ursachen von Verlust personenbezogener Daten festlegen, um diese Fälle zu verhindern. Die zu treffenden Vorbeugungsmaßnahmen müssen den Auswirkungen möglicher Problemsituationen angemessen sein.

Dieses Verfahren umfasst:

- Ermittlung potentieller Fehler und ihrer Ursachen,
- Beurteilung des Handlungsbedarfs, um das Eintreten von Datenverlusten, bzw. Fällen von Datenmissbrauch zu verhindern,
- Ermittlung und Verwirklichung der erforderlichen Maßnahmen,
- Abstimmung mit dem DSB über die erforderlichen Maßnahmen,
- Aufzeichnung der Ergebnisse der ergriffenen Maßnahmen,
- Bewertung der ergriffenen Vorbeugungsmaßnahmen.
- Es ist festzuhalten, wer was wann dokumentiert hat

Dokumentation

Der gesamte Prozess ist in der zeitlichen und tatsächlichen Reihenfolge zu dokumentieren.

Mitgeltende Unterlagen

- Art. 1, 2 und 10 des Grundgesetzes
- Richtlinie 95/45/EG vom 23.10.1995 (EU-DatSchRL)
- Richtlinie 2002/58/EG 12. Juli 2002 (EU-DSRL) (bis 24. Mai 2018)
- EU-Datenschutz-Grundverordnung (DS-GVO) Verordnung (EU) 2016/679 (ab 25. Mai 2018)
- Bundesdatenschutzgesetz (BDSG)
- Telekommunikationsgesetz (TKG) § 88, §§ 91 ff
- Informations- und Kommunikationsdienstgesetz (IuKDG)
- Sozialgesetzbuch (SGB I § 12, 35 Abs.4, SGB V § 301, SGB VIII §§ 61 Abs.4, 64 Abs.1, 67 Abs.6, 76, 102 Abs.2 Nr. 6, SGB X § 67b, 68, 71, 85, 100,)
- Betriebsverfassungsgesetz §§ 75 (2), 80 (1), 87 (1) 6 BetrVG
- StGB § 203

Verteilung (beispielhaft – dieser Verteiler ist entsprechend der Organisation der Beratungsstelle zu modifizieren)
– Vorstand
– Geschäftsführung
– Beraterinnen
– Büroleitung
– Datenschutzbeauftragter

7.4 IT – Sicherheitsrichtlinie

(Eine IT-Sicherheitsrichtlinie ist gemäß der EU-DSGVO ein Muss für Organisationen, die mit sensiblen personenbezogenen Daten arbeiten.)

Präambel

Ratsuchende der (Bezeichnung der Beratungsstelle), Mitarbeiter/-innen sowie Gäste und sonstige Besucher/-innen, Praktikant/-innen und Hospitant/-innen sowie Mitglieder des (Name des Trägers der Beratungsstelle) selbst sind in hohem Maße von der Informations- und Kommunikationstechnik und ihrem sicheren und zuverlässigen Funktionieren abhängig. Computer, Speichersysteme, Netzwerke und Daten sind wertvolle Ressourcen, deren Schutz für das Ansehen und den Geschäftserfolg des (Bezeichnung der Beratungsstelle) maßgeblich ist. Um diesen Schutz zu gewährleisten, hat der Vorstand die nachstehende IT-Sicherheitsleitlinie als Konkretisierung der Organisationsziele erlassen.

Geltungsbereich

Diese IT-Sicherheitsleitlinie gilt für den gesamten Tätigkeitsbereich des (Bezeichnung der Beratungsstelle). Sie enthält die Leitsätze für die IT-Sicherheit und die IT-Sicherheitsstrategie des (Bezeichnung der Beratungsstelle). Werden Dritte mit der Erbringung von Leistungen beauftragt, ist durch vertragliche Vereinbarungen sicher zu stellen, dass diese IT-Sicherheitsleitlinie in den Leistungsbeziehungen berücksichtigt wird.

Zweck

Die IT-Sicherheitsleitlinie des (Bezeichnung der Beratungsstelle) bildet die Grundlage für die Herstellung und den Erhalt des erforderlichen Sicherheitsniveaus für alle IT-Ressourcen im Verantwortungsbereich des (Bezeichnung der Beratungsstelle). Sie schafft und erhält das Bewusstsein der Mitglieder und Mitarbeiter/-innen für die IT-Sicherheit.

Bedeutung der IT-Sicherheit

Der Vorstand des (Bezeichnung der Beratungsstelle) misst der IT-Sicherheit eine hohe Bedeutung bei und fördert den IT-Sicherheitsprozess, welcher die Herstellung, den Erhalt, die Entwicklung und Fortschreibung des Sicherheitsniveaus umfasst. Alle Mitglieder und Mitarbeiter/-innen unterstützen den IT-Sicherheitsprozess im Rahmen ihrer jeweiligen Verantwortlichkeiten.

Verantwortung für die IT-Sicherheit

- Der Vorstand trägt die Verantwortung für die IT-Sicherheit im (Bezeichnung der Beratungsstelle).
- Die Führungskräfte (Vorstand, Regionalleitung etc.) verantworten die IT-Sicherheit jeweils für ihre Organisationseinheit (Bereich bzw. Abteilung).
- Das Herstellen und Erhalten der IT-Sicherheit liegt in der Verantwortung aller Mitglieder, Mitarbeiterinnen und Mitarbeiter.
- Die IT-Verantwortlichen setzen die Vorgaben dieser Leitlinie sowie die Vorgaben des Sicherheitskonzeptes kontinuierlich in geeigneter Weise um.

IT-Sicherheitsziele

Die Sicherheitsziele des (Bezeichnung der Beratungsstelle) sind:

- Informationen und Daten der Ratsuchende der (Bezeichnung der Beratungsstelle), Mitarbeiter/-innen sowie Gäste und sonstige Besucher/-innen, Praktikant/-innen und Hospitant/-innen sowie Mitglieder des (Name des Trägers der Beratungsstelle) sind gegen unberechtigte Kenntnisnahme und Veränderung sowie gegen Verlust geschützt, auch wenn sie keiner besonderen Geheimhaltung unterliegen. All diese Daten werden nach den erteilten Weisungen unter Berücksichtigung der gesetzlichen Vorgaben verarbeitet.

- Das (Bezeichnung der Beratungsstelle) gewährleistet grundsätzlich ein normales[25] Sicherheitsniveau im Sinne des BSI Grundschutzhandbuchs. Die dafür zu treffenden Maßnahmen werden entsprechend den gesetzlichen und vertraglichen Anforderungen unter Berücksichtigung der Wirtschaftlichkeit realisiert und dokumentiert.

- Die vom (Bezeichnung der Beratungsstelle) genutzte IT-Infrastruktur und die Daten sind durch technische und organisatorische Maßnahmen nach dem Stand der Technik vor Beschädigung, Zerstörung, Manipulation, Einschränkung oder Verlust ihrer Funktionalität und Vertraulichkeit geschützt.

- Ratsuchende der (Bezeichnung der Beratungsstelle), Mitarbeiter/-innen sowie Gäste und sonstige Besucher/-innen, Praktikant/-innen und Hospitant/-innen sowie Mitglieder des (Name des Trägers der Beratungsstelle) werden regelmäßig und bedarfsgerecht für die Belange der IT-Sicherheit sensibilisiert und geschult.

- Zur Erreichung der IT-Sicherheitsziele wird beim (Bezeichnung der Beratungsstelle) ein IT-Sicherheitsmanagement eingerichtet.

Unternehmensweite Sicherheitsregeln

Die nachstehenden Sicherheitsregeln sind stets zu beachten:

- Sicherheitsmaßnahmen für IT-Ressourcen und Daten sind hinsichtlich ihres Umfangs und ihrer Ausprägung auf Grund einer Risikobetrachtung so zu gestalten, dass höchstens ein beschriebenes und für vertretbar gehaltenes Restrisiko verbleibt. In der Regel erfolgt dies durch Herstellung und Erhalt des normalen IT-Sicherheitsniveaus nach dem BSI Grundschutzhandbuch.

- Bei der Erledigung fachlicher Aufgaben sind die spezifischen Anforderungen der IT-Sicherheit stets mit zu berücksichtigen.

- Für alle Prozesse beim (Bezeichnung der Beratungsstelle), die Berührungen mit der IT-Sicherheit oder Auswirkungen auf die IT-Sicherheit haben, sind von den fachlich zuständigen Stellen Festlegungen zu treffen und zu dokumentieren.

- Werden Sicherheitsanforderungen eines Ratsuchende der (Bezeichnung der Beratungsstelle), Mitarbeiter/-innen sowie Gästen und sonstigen Besucher/-innen, Praktikant/-innen und Hospitant/-innen sowie Mitglieder des (Name des Trägers der Beratungsstelle) realisierten Maßnahmen nicht erfüllt, so werden die zusätzlich erforderlichen Maßnahmen im Rahmen der technischen Möglichkeiten und der technischen Standards des (Bezeichnung der Beratungsstelle)- umgesetzt, wenn Ratsuchende der (Bezeichnung der Beratungsstelle), Mitarbeiter/-innen sowie Gäste und sonstige Besucher/-innen, Praktikant/-innen und Hospitant/-innen sowie Mitglieder des (Name des Trägers der Beratungsstelle) dies beauftragen.

Sicherheitsmanagement

Das Herstellen und Erhalten des IT-Sicherheitsniveaus ist eine Aufgabe aller Mitglieder, Mitarbeiterinnen und Mitarbeiter.

25 Im BSI-Grundschutzhandbuch werden drei Sicherheitsniveaus unterschieden, die mit gezielten Maßnahmen hinterlegt sind.

Organisation

Das IT-Sicherheitsmanagement-Team besteht aus einem Vertreter des Vorstandes, dem IT-Leiter, dem IT-Sicherheitsbeauftragten, dem Datenschutzbeauftragten und den IT-Sicherheitsmanagerinnen und –managern der Bereiche und Abteilungen. Die Aufgaben und Funktionen des IT-Sicherheitsbeauftragten, des Datenschutzbeauftragten und der IT-Sicherheitsmanagerinnen und –manager sind im IT-Sicherheits- und Datenschutz-Managementhandbuch gemeinsam mit der Organisations- und Kommunikationsstruktur näher beschrieben.

IT-Leiter

Der IT-Leiter unterstützt den Sicherheitsprozess fachlich und durch geeignete aktuelle Dokumentation des IT-Verbundes sowie seiner technischen Komponenten. Selbständig setzt er die Vorgaben der Leitlinie und des Sicherheitskonzeptes kontinuierlich um, leitet erforderliche zusätzliche Sicherheitsmaßnahmen zeitnah ein und kooperiert bei der Revision und/oder Auditierung des IT-Verbundes.

IT-Sicherheitsbeauftragte

Der IT-Sicherheitsbeauftragte ist für den IT-Sicherheitsprozess verantwortlich. Er leitet das IT-Sicherheitsmanagement. Er berichtet regelmäßig dem Vorstand. Soweit es dem IT-Sicherheitsbeauftragten aus Risikoerwägungen heraus geboten erscheint, hat er ein direktes Vortragsrecht beim Vorstand. Er arbeitet eng mit allen Leitungskräften. Bei Gefahr im Verzug handelt er verantwortungsbewusst zum Wohl des Unternehmens und ist dann in sicherheitsrelevanten Fragestellungen den IT-Sicherheitsmanagern gegenüber weisungsberechtigt.

IT-Sicherheitsmanager

IT-Sicherheitsmanagerinnen und -manager werden von der Geschäftsleitung für jeden Bereich bestellt. Sie sind für den IT-Sicherheitsprozess in ihrem Bereich verantwortlich. Sie berichten dem IT-Leiter und dem IT-Sicherheitsbeauftragten, unterstützen ggf. bei Audits und führen außerdem die Kundenkommunikation bei IT-Sicherheitsvorfällen und Notfällen durch. Aufgabenbündelungen sind zulässig.

Aufrechterhaltung des IT-Sicherheitsniveaus

IT-Sicherheitskonzepte

Für jedes Verfahren und IT-System, ggf. auch von Komponenten von IT-Systemen, werden die erforderlichen Sicherheitsmaßnahmen in einem IT-Sicherheitskonzept verbindlich beschrieben. Die IT-Sicherheitskonzepte werden regelmäßig durch den IT-Leiter, den IT-Sicherheitsbeauftragten sowie im Rahmen ihrer Bereiche die IT- Sicherheitsmanager auf ihre Aktualität und Wirksamkeit geprüft.

Verfahren bei Änderungen

Alle Änderungen an IT-Einrichtungen, -Verfahren oder -Prozessen, die vom (Bezeichnung der Beratungsstelle) betrieben werden, erfordern grundsätzlich eine Neubewertung der vorhandenen Sicherheitsmaßnahmen. Der IT-Sicherheitsbeauftragte ist schriftlich zu informieren.

Sicherheitsreviews (Sicherheits-Audits)

Der IT-Sicherheitsprozess des jeweiligen Bereichs wird von der IT-Sicherheitsmanagerin oder dem IT-Sicherheitsmanager, der übergreifende Prozess von der oder dem IT-Sicherheitsbeauftragten regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeiterinnen und Mitarbeitern bekannt, ob sie umgesetzt und in den Betriebsablauf integriert und wirksam bzw. warum sie nicht bekannt, nicht umgesetzt, nicht integriert oder nicht wirksam sind.

Sicherheitsvorfälle

Sicherheitsvorfälle sind Ereignisse, die im Widerspruch zu den dokumentierten Sicherheitszielen und -grundsätzen stehen, sowie Ereignisse, durch die nach Einschätzung von Mitgliedern, Mitarbeitern und Mitgliedern des (Bezeichnung der Beratungsstelle) Belange der IT-Sicherheit berührt werden. Dazu gehört auch die tatsächliche oder vermutete Bedrohung der Verfügbarkeit, Integrität oder Vertraulichkeit von IT-Systemen und Daten.

Erkennen Mitglieder, Mitarbeiterinnen oder Mitarbeiter Sicherheitsvorfälle, so sind sie verpflichtet, die IT-Abteilung und die Sicherheitsmanagerinnen und Sicherheitsmanager des betroffenen Bereichs bzw. der betroffenen Abteilung unverzüglich darüber zu informieren.

Sicherheitsvorfälle sind von den verantwortlichen Bereichen im Hinblick auf mögliche Auswirkungen zu untersuchen und zu bewerten. Auf Sicherheitsvorfälle ist mit Maßnahmen zu reagieren, die erforderlich und geeignet sind, die festgestellte Beeinträchtigung oder Abweichung von einer Festlegung zu beseitigen.

Der IT-Sicherheitsbeauftragte wirkt bei der Bearbeitung der Sicherheitsvorfälle mit. Die Bearbeitung kann nur mit seinem Einverständnis abgeschlossen werden.

IT-Sicherheits- und Datenschutz-Managementhandbuch

Im IT-Sicherheits- und Datenschutz-Managementhandbuch ist/wird festgelegt, auf welche Art und Weise diese Leitlinie implementiert wird.

Dazu sind insbesondere die Aufbauorganisation in der Form von Rollen und die Ablauforganisation als Prozess-Diagramme sowie deren Beziehungen untereinander beschrieben.

Bearbeitet von: DSB (T. Pudelko)

Kriterien	Schutzbedarf		
	normal	hoch	sehr hoch
Verstoß gegen Rechts-vorschriften, Verträge, internes Regelwerk	Verstöße mit geringfügigen Konsequenzen Haftungsschäden sind geringfügig	Verstöße mit erheblichen Konsequenzen Haftungsschäden sind erheblich	Fundamentaler Verstoß gegen Rechtsvorschriften Haftungsschäden sind existenzbedrohend
Verstoß gegen Datenschutz	Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als tolerabel eingeschätzt werden Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen	- Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich - Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen	- Eine gravierende Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten
Beeinträchtigung der persönlichen Unversehrtheit	Eine geringe Beeinträchtigung erscheint möglich	Eine nicht nur geringe Beeinträchtigung erscheint möglich	Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich - Gefahr für Leib und Leben
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden - Die tolerierbare Ausfallzeit ist größer als ein halber Arbeitstag	Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt - Die tolerierbare Ausfallzeit liegt zwischen einer Stunde und einem halben Arbeitstag	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden Die tolerierbare Ausfallzeit ist kleiner als eine Stunde
Negative Außenwirkung	Eine geringe Ansehens- oder Vertrauens-beeinträchtigung ist zu erwarten	Eine breite Ansehens- oder Vertrauens-beeinträchtigung ist zu erwarten	- Eine Ansehens- oder Vertrauensbeeinträchtigung in der Öffentlichkeit, evtl. sogar existenzgefährdender Art, ist denkbar
Finanzielle Auswirkungen	Der Schaden bewirkt geringe finanzielle Verluste Der finanzielle Schaden liegt unter 50.000 Euro	Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend Der finanzielle Schaden liegt zwischen 50.000 Euro und 200.000 Euro	Der finanzielle Schaden ist für die Institution existenzbedrohend Der finanzielle Schaden liegt höher als 200.000 Euro
Unberechtigte Offenlegung vertraulicher Informationen	Offenlegung von internen Date	Offenlegung von vertraulichen Daten	Offenlegung von streng vertraulichen Daten

Eine Vorabkontrolle ist dann durchzuführen, wenn besonders sensible Daten erhoben, gespeichert, verarbeitet, verändert, weitergegeben werden.

7.6 Checkliste zur Vorabkontrolle

1. Grundangaben		
geprüft		eigene Anmerkungen
☐	zur datenverarbeitenden Stelle	
☐	zur Zweckbestimmung	
☐	zur Rechtsgrundlage	
☐	zur Art der gespeicherten Daten	
zur Schutzbedürftigkeit der Daten, insb. bei sensitiven Daten i.S. v. § 4 BDSG oder sonst besonders schutzbedürftigen Daten		
☐	zum Kreis der Betroffenen	
☐	zur Übermittlung	
☐	zu den zugriffsberechtigten Personengruppen	
☐	zu den Fristen für die Löschung	

2. Prüfung		
geprüft	ob...	eigene Anmerkungen
☐	die Art der gespeicherten Daten	
☐	die Übermittlungen	
☐	die Eingrenzung der Zugriffsberechtigten	
☐	die Löschungsfristen	
von der angegebenen Zweckbestimmung und Rechtsgrundlage (Nr. 2) gedeckt sind. Ist dies nicht der Fall, muss geprüft werden, ob Änderungen im Verfahren möglich sind, die zu einem positiven Ausgang der Prüfung führen. Falls dies nicht möglich ist, ist die Alternative auszuschließen.		

3. Prüfung, ob die Rechte der Betroffenen gemäß BDSG gewahrt sind		
geprüft		eigene Anmerkungen
☐	Können die erforderlichen Auskünfte, Berichtigungen, Sperrungen und Löschungen durchgeführt werden?	
☐	Ist sichergestellt, dass der Betroffene seine Rechte ohne unvertretbaren Aufwand geltend machen kann?	

5. Beurteilung der möglichen Folgen bei missbräuchlicher Verwendung der Daten		
geprüft		eigene Anmerkungen
☐	Gefahren oder Nachteile für die Betroffenen	
☐	Schadensersatzansprüche	
☐	finanzielle Schäden	
☐	„Vertrauensschaden“	

6. Angaben zu der Technik des Verfahrens		
geprüft		eigene Anmerkungen
☐	Einzelplatz	
☐	bei vernetzten Rechnern auch Angaben zur Netzstruktur und Datenhaltung	
☐	eingesetzte Software	
☐	technische und organisatorische Maßnahmen	

Unterschrift der/des Vorgesetzten ……..

Unterschrift der ausfüllenden Person ……

7.7 Schweigepflichtentbindung

Die Schweigepflichtentbindung ist von der ratsuchenden Person auszufüllen und zu unterschreiben. Sie gilt für das Verhältnis von ratsuchender Person und Beraterin, um auf diese Person bezogene Informationen ggf. an die in der Schweigepflichtentbindung genannten Personen bzw. Institutionen weitergeben zu können, wenn dies dem Beratungszweck dient.

7.8. Datenschutzerklärung

Die Datenschutzerklärung ist von der Organisation, zu der die Beratungsstelle gehört bzw. dessen Träger zu erstellen und in angemessener Form (in der Regel als Teil des Impressum) zu veröffentlichen.

Generator zur Konfiguration einer Datenschutzerklärung: https://www.datenschutzexperte.de/datenschutz-muster/datenschutzerklaerung-konfigurator/

Schweigepflichtentbindungserklärung

Ich,

Frau, Herr

geboren am

Anschrift:

entbinde hiermit

(Name, Institution, Anschrift)

von der ihm/ihr obliegenden Schweigepflicht des § 203 Strafgesetzbuch (StGB)

gegenüber folgenden Personen/Institutionen:

1.

2.

3.

Die Entbindung von der Schweigepflicht umfasst alle Tatsachen und Erklärungen,

die ich (Name, Institution) gegenüber anvertraut habe.

Diese Entbindungserklärung kann ich jederzeit schriftlich zurücknehmen.

....
Datum Unterschrift

Name:

Vor Beginn einer Tätigkeit als Berater/-in ist eine Verpflichtungserklärung von dem/der angehenden Berater/-in auszufüllen und zu den Personalakten zu nehmen. Es ist darauf zu achten, dass der/die angehende Berater/-in das dazugehörige Merkblatt erhält, gelesen und verstanden hat.

7.9 Verpflichtungserklärung nach § 5 des Bundesdatenschutzgesetzes (BDSG) zur Wahrung des Datengeheimnisses

.....

Name der verantwortlichen Stelle

Sehr geehrte(r) Frau/Herr.....

aufgrund Ihrer Aufgabenstellung verpflichte ich Sie auf die Wahrung des Datengeheimnisses nach § 5 BDSG. Es ist Ihnen nach dieser Vorschrift untersagt, unbefugt personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen.

Diese Verpflichtung besteht auch nach Beendigung Ihrer Tätigkeit fort.

Verstöße gegen das Datengeheimnis können nach §§ 44, 43 Absatz 2 BDSG sowie nach anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden.

In der Verletzung des Datengeheimnisses kann zugleich eine Verletzung arbeits- oder dienstrechtlicher Schweigepflichten liegen.

Eine unterschriebene Zweitschrift dieses Schreibens reichen Sie bitte an die Personalabteilung zurück.

....

Ort, Datum Unterschrift der verantwortlichen Stelle

Über die Verpflichtung auf das Datengeheimnis und die sich daraus ergebenden Verhaltensweisen wurde ich unterrichtet. Das Merkblatt zur Verpflichtungserklärung (Texte der §§ 5, 43 Absatz 2, 44 BDSG) habe ich erhalten.

....

Ort, Datum Unterschrift des Verpflichteten

Merkblatt zur Verpflichtungserklärung

§ 5 BDSG – Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nichtöffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 43 Absatz 2 BDSG – Bußgeldvorschriften

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,

5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt,

5a. entgegen § 28 Abs. 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,

5b. entgegen § 28 Abs. 4 Satz 1 Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt,

6. entgegen § 30 Abs. 1 Satz 2, § 30a Abs. 3 Satz 3 oder § 40 Abs. 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder

7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

§ 44 BDSG – Strafvorschriften

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Aufsichtsbehörde.

8 Links

Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/it_grundschutzstandards.html

Allgemeine Informationen zum Thema Datenschutz und Datenschutzbeauftragte
https://www.datenschutzbeauftragter-info.de/

Gesetze im Internet
https://www.gesetze-im-internet.de/

Die EU-Datenschutzgrundverordnung
https://dsgvo-gesetz.de/

Zu Verschlüsselungstechnologien
https://www.bsi.bund.de/DE/Themen/Kryptotechnologie/kryptotechnologie_node.html

Sichere Passwörter
https://www.sicher-im-netz.de/dsin-muster-passwortkarte

Sichere Aktenschränke
http://betriebseinrichtung.net/aktenschraenke-alles-sicher-unter-verschluss/

Schulungen, Seminare und Qualitäts-Checks PQ-Sys® plus
http://www.der-paritaetische.de/service

DER PARITÄTISCHE
GESAMTVERBAND

Oranienburger Str. 13-14
10178 Berlin
Tel. 030-2 46 36-0
Fax 030-2 46 36-110

www.paritaet.org
info@paritaet.org