Datenschutzkonzept EUTB in der Landesarbeitsgemeinschaft Selbsthilfe Brandenburg

Dieser Text ist nur in männlicher Sprache geschrieben. Zum Beispiel steht im Text nur das Wort Mit-Arbeiter. Das Wort Mit-Arbeiterinnen steht nicht im Text. Mit-Arbeiter können aber auch Frauen sein. Wir wollen mit dieser Sprache niemanden verletzen. Frauen sind uns genauso wichtig wie Männer. Wir machen das so, damit man den Text besser lesen kann.

Inhalt

1 Ziele des Datenschutzkonzeptes 3
2 Geltungsbereich 3
3 Rechtsgrundlagen des Datenschutzes 3
4 Datenschutzgrundsätze 4
4.1 Begriffe 4
4.2 Grundsätze 4
5 Verantwortlichkeiten in der Datenschutzorganisation 5
5.1 Verantwortlicher 5
5.2 Leitung 5
5.3 Datenschutzbeauftragter 5
5.4 Personalverantwortliche 6
5.5 IT-Verantwortliche 7
5.6 Mitarbeiter 7
6 Organisation des Datenschutzes in der EUTB-Beratungsstelle 7
6.1 Betroffene Personen 7
6.2 Personenbezogene Daten 7
6.3 Verfahrensbeschreibungen 8
6.4 Sensibilisierung/ Schulungskonzept 9
6.5 Folgenabschätzung und Risikomanagement 9
6.5.1 Datenschutz-Folgenabschätzung 9
6.5.2 Risikomanagement 10
7 Datenschutzmaßnahmen 10
7.1 Vertraulichkeit 11
7.2 Integrität 11
7.3 Verfügbarkeit und Belastbarkeit 11
7.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung 11
8 Datenschutzvorfälle und Anfragen 12
9 Kontinuierlicher Verbesserungsprozess 13
10 Abkürzungsverzeichnis 14
11 Anhänge 15
11.1 Was Sie beachten müssen, wenn…. 15

1 Ziele des Datenschutzkonzeptes

Der Schutz von personenbezogenen Daten ist für die Landesarbeitsgemeinschaft Selbsthilfe Brandenburg e.V wichtig. Mit Datenschutz soll das Recht auf informationelle Selbstbestimmung geschützt werden. Dieses Grundrecht ist als Ausprägung des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Dafür sind Regelungen zum Umgang mit den Daten nötig.

Mit den personenbezogenen Daten soll vertraulich umgegangen werden.

Das Konzept hilft beim Vorgehen im Datenschutz. Mit den Regeln gewinnen die Mitarbeiter Sicherheit. Sie sollen sich daran orientieren. Es zeigt, welche Anforderungen einzuhalten sind.

Es zeigt wie der Datenschutz im Unternehmen organisiert wird. Dazu gehört:

- wer etwas tun muss (zum Beispiel: Mitarbeiter oder Leitung),
- was die Person für den Datenschutz tun muss (welche Aufgaben und Maßnahmen),
- was alle Mitarbeiter beachten müssen (Regeln).

Ziel ist es bei den Regeln,

- die aktuellen Gesetze zum Datenschutz zu erfüllen und
- auf die Arbeit in den Beratungsstellen zu übertragen.

2 Geltungsbereich

Die Regeln gelten für alle Mitarbeiter der Beratungsstelle *der Unabhängigen ergänzenden Teilhabeberatungsstelle.*

Anwenden sollen diese Regeln alle Beratungsstellen. Sie gelten für Beratungsstellen ab einem Mitarbeiter.

3 Rechtsgrundlagen des Datenschutzes

Für die Beratungsstelle sind Anforderungen der folgenden Rechtsgrundlagen zu beachten:

- Bundesdatenschutzgesetz (im Folgenden: BDSG) alte Fassung (im Folgenden: a. F.) und neue Fassung (im Folgenden: n. F.), die neue Fassung gilt ab dem 25.5.2018
- EU-Datenschutzgrundverordnung (im Folgenden: DSGVO), die ab dem 25.5.2018 gilt.

Im Rahmen dieses Konzeptes werden die neuen Rechtsgrundlagen ab dem 25.5.2018 angewandt.

Weitere Normen sind wichtig:

- zum Sozialdatenschutz, Teile des Sozialgesetzbuchs, zum Beispiel das erste Buch, neunte Buch und zehnte Buch (im Folgenden: SGB I, SGB IX, SGB X),
- zur Verletzung von Privatgeheimnissen das Strafgesetzbuch (StGB)
- für die Telekommunikation das Telekommunikationsgesetz (TKG), zum Beispiel zum unerlaubten Abhören,
- für die Telemedien das Telemediengesetz (TMG), zum Beispiel in Bezug auf die Internetseite,
- für den Schutz im Bereich der elektronischen Kommunikation die ePrivacy-Verordnung, die mit der DSGVO ab 25.5.2018 wirksam werden soll,
- zum Umgang mit Fotos das Kunst-Urhebergesetz (KunstUrG),

- für den Arbeitnehmerdatenschutz das Betriebsverfassungsgesetz (BtrVG), zum Beispiel für Mitarbeitervertretungen
- für das Aufbewahren von Daten die Pflichten zur Aufbewahrung, zum Beispiel aus der Abgabenordnung (AO, steuerrechtlich) und dem Handelsgesetzbuch (HGB, handelsrechtlich).

Bei dem BDSG n. F. und der DSGVO handelt es sich um subsidiäre (nachrangige) Regelungen. Das bedeutet sie treten gegenüber spezielleren Regelungen, zum Beispiel für soziale Bereiche (§§67 ff SGB X), zurück.

4 Datenschutzgrundsätze

4.1 Begriffe

Im Art. 4 der DSGVO sind zahlreiche Begriffe für das Datenschutzrecht definiert (siehe: https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf (Datenschutz-Grundverordnung, Seite 44). Sie helfen, das Recht zu verstehen.

Wesentliche Punkte werden hier vereinfacht beschrieben.

Eine „betroffene Person“ ist eine natürliche Person, von der Daten verarbeitet werden. Die betroffene Person hat Rechte (siehe 6.1).

„Personenbezogene Daten“ sind die Informationen von einer natürlichen Person. Mit den Daten kann man auf die Person schließen. Dazu sagt man, sie ist identifizierbar. Das kann direkt durch den Namen passieren. Auch einzelne Informationen ohne Namen können auf eine Person schließen lassen, zum Beispiel eine Adresse.

Zu den „Besonderen Kategorien personenbezogener Daten“ zählen nach Art. 9 DSGVO unter anderem Gesundheitsdaten (siehe auch 6.2).

„Verarbeiten“ bedeutet das Vorgehen im Zusammenhang mit den personenbezogenen Daten. Das kann digital und in Papierform sein. Dazu zählt bei der Arbeit in der Beratungsstelle zum Beispiel, wenn personenbezogene Daten:

- erfasst werden,
- gespeichert werden,
- gedruckt werden,
- weitergeleitet werden,
- gelöscht werden.

„Pseudonymisierung“ bedeutet, dass die personenbezogenen Daten ohne zusätzliche Informationen (eine Art Schlüssel) nicht mehr eindeutig einer betroffenen Person zugeordnet werden können. Diese zusätzlichen Informationen müssen nach den Anforderungen des Datenschutzes aufbewahrt werden.

Bei der „Anonymisierung“ werden personenbezogene Daten so verändert, dass sie nicht mehr einer Person zugeordnet werden können. Anonymisierte Daten unterliegen nicht dem Datenschutz.

„Sozialdaten“ sind personenbezogene Daten, die von einer Stelle, die dem Sozialgeheimnis unterfällt, im Hinblick auf ihre Aufgaben nach dem Sozialgesetzbuch verarbeitet werden (siehe § 67 Absatz 2 Satz 1 SGB X).

4.2 Grundsätze

Die EU hat in der DSGVO die wichtigsten Punkte im Datenschutz zusammengefasst. Das nennt man Grundsätze. Die Grundsätze finden sich im Art. 5 der DSGVO, (siehe:

https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf
(Datenschutz-Grundverordnung, Seite 52).

Die DSGVO verlangt, dass sie beim Umgang mit personenbezogenen Daten beachtet werden. Die Grundsätze sind wie ein Fundament, worauf das Handeln im Datenschutz aufbaut.

Die wesentlichen Punkte sind:

- Rechtmäßigkeit, d. h. dass es muss grundsätzlich eine Erlaubnis geben für das Verarbeiten (zum Beispiel ein Gesetz, siehe unter 3. oder eine Einwilligung).
- Transparenz, d. h. das Arbeiten mit den personenbezogenen Daten muss nachvollziehbar sein (zum Beispiel, woher kommen Daten, wo werden sie gespeichert, wohin werden sie weitergeleitet).
- Zweckbindung, d. h. es ist für jede Verarbeitung ein Grund zu bestimmen. Daten dürfen nicht für einen anderen Zweck verwendet werden.
- Datenminimierung, d. h. dass nur so viele Daten wie nötig verarbeitet werden. Die Grundsätze Datenvermeidung und Datensparsamkeit aus dem BDSG a.F. werden zukünftig mit Datenminimierung zusammengefasst.
- Richtigkeit, d. h. die Daten müssen stimmen. Sind sie falsch, müssen sie berichtigt oder gelöscht werden.
- Speicherbegrenzung, d. h. die Daten müssen gelöscht werden, wenn sie nicht gebraucht werden.
- Integrität, d. h. die Daten dürfen nicht von Unbefugten verändert werden.
- Vertraulichkeit, d. h. die Daten müssen vertraulich behandelt werden. Unbefugte dürfen sie nicht einsehen.
- Rechenschaftspflicht, d. h. der Verantwortliche muss die genannten Punkte zum Umgang mit den Daten einhalten und dies nachweisen können.

5 Verantwortlichkeiten in der Datenschutzorganisation

Alle Mitarbeiter und die Leitung sind in gleichem Maße verantwortlich im Datenschutz und müssen die Gesetze und Regeln einhalten.

5.1 Verantwortlicher

Der Verein „Landesarbeitsgemeinschaft Selbsthilfe Brandenburg e.V“, ist

- laut Art. 4 Nr. 7 DSGVO „Verantwortlicher“. Er entscheidet über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten.

5.2 Leitung

Die Leitung

- bestimmt verantwortliche Personen und
- schafft die Voraussetzungen, die Regeln einzuhalten
- muss dafür sorgen, dass den Mitarbeitern die Regeln vertraut werden
- bestellt und unterstützt den Datenschutzbeauftragten.

5.3 Datenschutzbeauftragter

Die DSGVO bestimmt, dass unter bestimmten Bedingungen ein betrieblicher Datenschutzbeauftragter bestellt werden muss. Die Bedingungen sind im Art. 37 DSGVO benannt (siehe:
https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf,
(Datenschutz-Grundverordnung, Seite 105). Einen Datenschutzbeauftragten muss jedes Unternehmen bestellen, wenn es Tätigkeiten nachgeht, die einer besonderen Kontrolle unterliegen,

- wenn die Kerntätigkeit in der „umfangreichen Verarbeitung besonderer Kategorien von Daten“ besteht. (siehe auch Punkt 6.1)

Es kann ein Mitarbeiter mit der erforderlichen Fachkunde oder ein externer Datenschutzbeauftragter bestellt werden. Der kommissarische betriebliche Datenschutzbeauftragte des Vereins „Landesarbeitsgemeinschaft Selbsthilfe Brandenburg e.V.“ ist, sowie der Datenschutzbeauftragte der Beratungsstelle:

Herr Mathias Hecht,

Telefonnummer: 03332 521751

E-Mailadresse Datenschutzbeauftragter: Datenschutz@lag-selbsthilfe-bb.de

Der Beauftragte arbeitet als Stabsstelle zur Geschäftsleitung,

- verfügt über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren und
- überwacht die Einhaltung der Bestimmungen der DSGVO
- unterstützt die Leitung,
- wirkt auf die Umsetzung der Datenschutzanforderungen hin
- ist Ansprechpartner für Fragen in dem Bereich, für Mitarbeiter und Ratsuchende
- sollte das Datenschutzkonzept mindestens einmal im Jahr überprüfen und es bei Bedarf anpassen.

Der Datenschutzbeauftragte führt die Sensibilisierung der Mitarbeiter durch bzw. ist für die Organisation verantwortlich. Er dokumentiert Datenschutzschulungen und bewahrt Nachweise dafür auf.

Bei der Festlegung und Umsetzung der technischen und organisatorischen Maßnahmen unterstützt der Datenschutzbeauftragte. Er steht in engem Austausch mit den Verantwortlichen und berichtet der Geschäftsleitung.

Das regelmäßige Überprüfen und Aktualisieren der Datenschutzdokumente (siehe Anhang) übernimmt der Datenschutzbeauftragte. Ziel ist es, dass diese den tatsächlichen Abläufen entsprechen.

5.4 Personalverantwortliche

Personalverantwortliche halten im Bewerberauswahlprozess und bei der Personaldatenführung alle Datenschutzanforderungen ein. Die Aufbewahrungs- und Löschfristen unterscheiden sich von anderen Abläufen und sind zu beachten. (siehe Dokument im Anhang)

Die Personalverantwortlichen im Unternehmen organisieren die Einweisung im Datenschutz. Jeder Mitarbeiter muss vor Tätigkeitsbeginn mit den Belangen des Datenschutzes vertraut gemacht werden.

Die Personalverantwortlichen sorgen dafür, dass die „Verpflichtung zur Vertraulichkeit“ sowie die Verpflichtung auf das Sozialgeheimnis Teil des Arbeitsvertrages werden -. (siehe Anlage). Bei Tätigkeitsende weist der Personalverantwortliche darauf hin, dass die Verpflichtung zur Vertraulichkeit auch nach dem Ende der Beschäftigung gilt.

Die Nachweise dazu werden in der Personalakte dokumentiert.

Für die Beantragung der erforderlichen Zugriffsrechte bei den IT-Verantwortlichen sind die Personalverantwortlichen zuständig.

5.5 IT-Verantwortliche

Die IT-Verantwortlichen müssen in ihrer Aufgabe besonders im Bereich Datenschutz sensibilisiert werden. Sie nehmen im Unternehmen eine wichtige Funktion ein und sind für das Umsetzen der technischen Voraussetzungen verantwortlich.

Die IT-Verantwortlichen unterstützen den Datenschutzbeauftragten bei technischen Informationen zu den Abläufen. Für die datenschutzrechtliche Bewertung von Verfahren, wie der Folgenabschätzung, ist es u.a. wesentlich zu erfahren

- wo Daten gespeichert werden,
- wie die Vertraulichkeit, Verfügbarkeit und Integrität gewährleistet ist,
- wie die vertrauliche Übermittlung gesichert ist,
- wie die Benutzerverwaltung (Anlegen der Mitarbeiter in Softwarelösungen) erfolgt,
- auf welche Weise Zugriffsrechte vergeben werden.

5.6 Mitarbeiter

Alle Mitarbeiter unterschreiben als Anhang zum Arbeitsvertrag eine Verpflichtung zur Vertraulichkeit. Das beinhaltet einerseits die Verpflichtung auf das Datengeheimnis nach § 5 BDSG. Die Verpflichtung gilt auch über das Ende der Tätigkeit hinaus. Über die Schweigepflicht nach § 203 StGB (Verletzung von Privatgeheimnissen) werden sie aufgeklärt. Auf die Wahrung des Sozialgeheimnisses nach § 35 SGB I werden die Mitarbeiter verwiesen.

Die Mitarbeiter müssen zu Beginn des Arbeitsverhältnisses und dann regelmäßig mit den Belangen des Datenschutzes vertraut gemacht werden. Dazu gehören praktische Maßnahmen im Alltag.

Die Regeln und Maßnahmen zum Schutz vor unbefugtem Zugriff müssen sie einhalten. D.h. die personenbezogenen Daten dürfen nicht in falsche Hände geraten. Sie müssen die Leitung informieren, wenn sie von dem Verlust oder einem Verstoß erfahren.

6 Organisation des Datenschutzes in der EUTB-Beratungsstelle

6.1 Betroffene Personen

In den Beratungsstellen sind folgende Personen von der Verarbeitung betroffen:

- die Beschäftigten: Beschäftigte sind alle, die für die EUTB tätig sind. Dazu gehören auch Ehrenamtliche, Praktikanten, studentische Hilfskräfte, Auszubildende, Bewerber (§ 26 BDSG neue Fassung). Im Rahmen der Tätigkeit werden Informationen zu ihnen bekannt, zum Beispiel durch die Dokumentation der Beratung oder im Zusammenhang mit den Personalabläufen.

- Ratsuchende: Das sind die Personen, die die Beratung nutzen und in Anspruch nehmen. Die Dokumentation dieser Personen erfolgt im großen Umfang und ist Hauptaufgabe der Beratung zur Teilhabe.

- Externe Ansprechpartner: Dazu zählen zum Beispiel Angehörige, gesetzliche Betreuer, Interessenten, Berater der Fachstelle Teilhabeberatung. Hinweise zu diesen Personen können im Laufe der Beratung notwendig sein.

6.2 Personenbezogene Daten

Wesentlich ist, dass bei der Haupttätigkeit in den Beratungsstellen durch die Beschäftigten Daten mit besonderem Schutzbedarf verarbeitet werden.

Personenbezogene Daten können nach Schutzstufenkonzepten in Schutzbedarfskategorien eingeteilt werden. Üblicherweise gibt es den Schutzbedarf „niedrig“ oder „gering“, „mittel“, „hoch“ und „sehr hoch“. Verwendet werden auch nur drei Stufen: „normal“, „hoch“ und „sehr

hoch“ (siehe https://www.datenschutz-praxis.de/praxishilfen/download-uebersicht-schutzstufenkonzepte/). Die Bestimmung des Schutzbedarfs der personenbezogenen Daten hängt z.B. davon ab,

- ob die Daten für Dritte einen besonderen Wert darstellen
- wie sensibel die personenbezogenen Daten im jeweiligen Verfahren sind
- wie groß der Umfang der verarbeiteten personenbezogenen Daten ist
- ob die Anwendung, mit der verarbeitet wird, besonders kritisch ist
- ob unbeabsichtigter oder unrechtmäßiger unbefugter Zugriff (Vernichtung, Verlust, Veränderung, Offenlegung) zu physischen, materiellen oder immateriellen Schaden führen kann
- ob das jeweilige System/Verfahren in der Öffentlichkeit steht und ein Reputationsschaden droht?

Die in der Beratungsstelle verarbeiteten personenbezogenen Daten sind hinsichtlich der Grundrechte und Grundfreiheiten der betroffenen Personen besonders sensibel. Es findet eine umfangreiche Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DSGVO statt. In Abhängigkeit des jeweiligen Verfahrens können die personenbezogenen Daten einen hohen Schutzbedarf haben. Bei dem Nutzen einer Telefonnummer und des Namens liegt beispielsweise ein geringerer Schutzbedarf vor als bei der Erstellung einer Beratungsdokumentation mit allen sozialen und gesundheitlichen Hintergrundinformationen. Bei einem Großteil der Verfahren wird ein hoher Schutzbedarf angenommen.

Für die Verarbeitung sensibler personenbezogener Daten gelten erhöhte Anforderungen, wie die Bestellung des Datenschutzbeauftragten (siehe 5.2) und die Datenschutz-Folgenabschätzung (siehe 6.5.1). Der Schutzbedarf der jeweiligen Daten eines Verfahrens wird im Risikomanagement (siehe 6.5.2) berücksichtigt und hat einen Einfluss auf die Planung der Maßnahmen (siehe 7).

Ein Personenbezug ergibt sich, wenn die betroffene Person identifizierbar ist. Eine Person ist identifizierbar mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standorten. Es kann sich auch um Merkmale handeln, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind und weshalb sie identifiziert werden kann.

Laut Art. 9 DSGVO werden während der Beratung besondere Kategorien personenbezogener Daten verarbeitet. Dazu gehören zum Beispiel ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Art. 4 DSGVO definiert Gesundheitsdaten. Die personenbezogenen Daten beziehen sich auf körperliche oder geistige Gesundheit einer natürlichen Person. Es sind Informationen, aus denen der Gesundheitszustand hervorgeht.

Der Sozialdatenschutz findet Anwendung. Zu den verarbeiteten Daten in der Beratungsstelle zählen Sozialdaten laut § 67 SGB X.

6.3 Verfahrensbeschreibungen

Der Datenschutzbeauftragte dokumentiert fortlaufend alle Verfahren, in denen personenbezogene Daten verarbeitet werden und bewertet sie (siehe auch 5.2 und 6.5). Es gibt ein s. g. Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO. Dies enthält die Punkte, die nach DSGVO enthalten sein müssen (siehe

https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf, (Datenschutz-Grundverordnung, Seite 93).

Die Übersicht beschreibt, welche personenbezogenen Daten, zu welchem Zweck, mit welchem automatisierten Verfahren (Softwarelösung/Anwendung), auf welche Weise, durch wen verarbeitet werden und welche Datenschutzmaßnahmen dabei getroffen wurden. Hierin wird auch aufgeführt, wenn eine Verarbeitung personenbezogener Daten durch Subunternehmen im Auftrag stattfindet. Die vollständig ausgefüllte Verfahrensbeschreibung ist dem Datenschutzbeauftragten zur Aufnahme in das Verzeichnis der Verarbeitungstätigkeiten zu übermitteln.

Die Fachstelle Teilhabeberatung hat zum Start der Tätigkeit in der Beratungsstelle zahlreiche Datenschutzdokumente erstellt. Sie sind im Anhang dieses Konzeptes aufgeführt. Teilweise können sie für die Verfahrensbeschreibungen in dem Verzeichnis von Verarbeitungstätigkeiten herangezogen werden. Die Dokumente gelten mit diesem Konzept und sind durch jeden Mitarbeiter im Beratungsprozess zu beachten. Für die einzelnen Arten der Beratung sind darin spezielle Hinweise im Datenschutz berücksichtigt. Die unterschiedliche Art der Datenübermittlung hat z.B. einen wesentlichen Einfluss auf die getroffenen Datenschutzmaßnahmen. So gelten für die Telefonberatung andere Anforderungen als für die Beratung per Mail.

6.4 Sensibilisierung/ Schulungskonzept

Es ist wichtig, dass allen Mitarbeitern der Datenschutz und die Maßnahmen dafür bei der täglichen Arbeit bewusst sind (gemäß Art. 32 Abs. 4 DSGVO). Jeder Mitarbeiter soll über den gleichen Wissensstand verfügen. Ein wesentlicher Bestandteil dafür ist die Schulung der Mitarbeiter im Datenschutz. Die Schulungen finden zu Beginn der Tätigkeit und dann regelmäßig statt, um das Datenschutzniveau aufrechtzuerhalten bzw. zu steigern. Die Inhalte der Schulungen müssen an Veränderungen durch Gesetze oder technische Entwicklungen sowie in Abhängigkeit der Abläufe im Unternehmen angepasst werden. Der Datenschutzbeauftragte überprüft den Erfolg der Schulungsmaßnahmen und bezieht die Ergebnisse in die neuen Schulungen ein.

6.5 Folgenabschätzung und Risikomanagement

6.5.1 Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung ist erforderlich, um spezifische Risiken der automatisierten Verarbeitung personenbezogener Daten zu minimieren. Im § 4 d BDSG a.F. heißt dieser Vorgang Vorabkontrolle.

Der Verantwortliche nimmt vor der Einführung neuer Verfahren, bei denen in besonderem Umfang sensible personenbezogene Daten betroffen sind, eine Datenschutz-Folgenabschätzung nach Art. 35 Abs. 3 DSGVO (siehe https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf, (Datenschutz-Grundverordnung, Seite 99) vor. Er sollte den Datenschutzbeauftragten mit einbeziehen. Der Verantwortliche dokumentiert und bewertet das Verfahren laut Art. 35 Abs. 7 DSGVO. Es müssen folgende Punkte mindestens enthalten sein:

- Beschreibung der geplanten Verarbeitungsvorgänge
- Zweck der Verarbeitung
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen (siehe 6.1 und 6.2)
- die Abhilfemaßnahmen zur Bewältigung der Risiken (Sicherheitsvorkehrungen, Verfahren, die sicherstellen und nachweisen, dass die DSGVO eingehalten wird).

- Entsprechend der Risiken werden die geeigneten technischen und organisatorischen Maßnahmen vom Datenschutzbeauftragten getroffen.

Wenn sich erkannte Risiken nicht hinreichend behandeln lassen, darf das Verfahren nicht zum Einsatz kommen.

Ergebnis und die Begründung sind zu dokumentieren. Die verantwortliche Stelle ist für die erforderlichen Informationen verantwortlich. Die IT-Verantwortlichen werden ggf. einbezogen (siehe 5.3).

6.5.2 Risikomanagement

Ein Risiko ist die Möglichkeit, dass eine vorhandene Bedrohung eine Schwachstelle eines Wertes ausnutzt und dadurch dem Unternehmen Schaden zufügen könnte.

Das Risikomanagement ist für alle Datenschutzverfahren relevant (siehe 6.3).

Gemäß Art. 32 Abs. 1 DSGVO (siehe https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf, (Datenschutz-Grundverordnung, Seite 95) ist für das Bestimmen der technischen und organisatorischen Maßnahmen das Risiko für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Für die Einschätzung des Risikos ist das Schutzniveau einzubeziehen. Dafür ist der Schutzbedarf der jeweiligen personenbezogenen Daten innerhalb eines Verfahrens festzulegen (siehe 6.2).

Der Datenschutzbeauftragte trifft zusammen mit den Verantwortlichen des Verfahrens, der IT und der Geschäftsführung die Abwägung und analysiert und bewertet Risiken.

Beeinflusst wird die Einstufung durch die Eintrittswahrscheinlichkeit und die Schwere des potentiellen Schadens. Ein Schaden kann entstehen, wenn personenbezogene Daten z.B. unbeabsichtigt

- vernichtet werden,
- verändert werden,
- verloren gehen,
- unbefugt offengelegt werden
- Unbefugte Zugang erlangt haben. (Art. 32 Abs. 2 DSGVO)

Der Datenschutzbeauftragte

- dokumentiert analysierte Risiken,
- das Schadenspotential,
- bewertet es,
- legt Maßnahmen zur Behandlung des Risikos fest,
- stimmt sie mit den Verantwortlichen ab und
- dokumentiert das voraussichtliche Restrisiko.

7 Datenschutzmaßnahmen

Laut Art. 32 Abs. 1 DSGVO sind geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Zu diesen Maßnahmen zählen laut DSGVO allgemein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste auf Dauer sicherzustellen,
- die Fähigkeit, die Verfügbarkeit und den Zugang zu ihnen bei einem physischen und technischen Zwischenfall rasch wiederherzustellen,

- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Aufgrund dessen gelten allgemeine Standards für alle Beratungsstellen, die Unbefugten den Zugang zu personenbezogenen Daten verwehren sollen. Die Maßnahmen beziehen sich auf Papierakten und die digitalen Daten in gleichem Maße.

Auf der Grundlage sind wesentliche Maßnahmen innerhalb der Beratungsstelle getroffen und müssen eingehalten werden. Nachfolgende Maßnahmen sind nicht als abschließend und allumfassend anzusehen. Sie sind eine grundlegende Auswahl. Die Maßnahmen hängen u. a. von den Gegebenheiten der Beratungsstelle ab (z. B. der Größe).

Die Punkte 7.1 und 7.2 betreffen alle Mitarbeiter, der Punkt 7.3 eher IT-Verantwortliche und 7.4 das Management.

7.1 Vertraulichkeit

- Nutzen der Zutrittsmittel nur entsprechend der Rechte und Aufgabenerfüllung
- Verschließen aller personenbezogenen Unterlagen im abschließbaren Schrank nach Geschäftszeit (clean desk)
- Nutzen neutraler Räume für vertrauliche Gespräche
- Verwenden sicherer Passwörter
- Sperren des Bildschirms bei Verlassen des Arbeitsplatzes
- Einhalten von Regelungen zum mobilen Arbeiten (keine lokale Speicherung, verschlüsselte Laptops)
- Physische und logisches Trennen von Daten zu unterschiedlichen Zwecken (nach Team, nach Bearbeiter, nach Nutzer)
- Einhalten der Regelungen zum ordnungsgemäßen Löschen
- Nutzen eines Schredders nach DIN 66399 mit der geforderten Sicherheitsstufe 4
- Erteilen von Auskunft gegenüber der betroffenen Person oder gegenüber Externen nur nach internen Regeln
- Hinzuziehen der Leitung und des Datenschutzbeauftragten bei Fragen, Einhalten der Meldewege (siehe 8)

7.2 Integrität

- Einhalten der Prozesse zum Schaffen der Rechtsgrundlage für die Verarbeitung (Einwilligung, Schweigepflichtsentbindung, siehe Dokumente im Anhang)
- Weitergabe von Informationen zur Verarbeitung gg. der betroffenen Person (Transparenz, Informationspflicht)
- Anonymisieren und Pseudonymisieren, wo möglich
- Sicher Daten versenden und weitergeben nach den internen Regeln
- Protokollierung der Verarbeitung (Transparenz, wer hat wann, was verarbeitet)
- Regelungen einhalten im Umgang mit externen Speichermedien

7.3 Verfügbarkeit und Belastbarkeit

- Einhalten der technischen Prozesse in der IT zur Verfügbarkeit (Firewall, Virenschutz, USV, Verschlüsselung von externen Speichermedien usw.)
- Prozess zur regelmäßigen Datensicherung einhalten

7.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Schaffen eines Prozesses zu Schlüsselregelungen (Vergabe /Entzug)
- Schaffen und Dokumentieren von Zutrittsbereichen (Empfang, Wartebereich, Beratungsraum)
- Vergabe und Dokumentation der Zutrittsberechtigungen entsprechend der Aufgabenerfüllung

- Vergabe der Schlüssel für die Schränke entsprechend der Aufgabe (Trennung im Team)
- Schaffen von Regelungen zum Aufbewahren mit Anweisungen zur Speicherdauer sowie zu Löschfristen
- Schaffen einer Übersicht über die Datenverarbeitungsprogramme und Datenflüsse (siehe 6.3)
- Einrichten eines Prozesses zur Vergabe/zum Entzug mit Dokumentation der Zugriffsrechte, Benutzerverwaltung (Need to know, Berechtigungskonzept)
- Technisches Erzwingen von Passwortregeln
- Einrichten eines Prozesses für Passwortneuvergabe
- Festlegen von Möglichkeiten der Verschlüsselung (Austauschorder, ZIP)
- Schaffen von Regelungen zum mobilen Arbeiten (keine lokale Speicherung, verschlüsselte Laptops)
- Schaffen von Reglungen zum Umgang mit externen Speichermedien (USB…)
- Schaffen der Voraussetzungen zur Nachweisbarkeit im Umgang mit den Daten
- Verträge mit externen Dienstleistern im Rahmen der Auftragsverarbeitung
- Regelmäßige Überprüfung der Maßnahmen durch interne Audits
- Einrichten eines Prozesses zum Wiederherstellen von Daten (Datensicherung)
- Technische Prozesse zur Verfügbarkeit (Firewall, Virenschutz, USV usw.) einführen, umsetzen und aufrechterhalten

8 Datenschutzvorfälle und Anfragen

Datenschutzvorfälle sind unverzüglich dem Datenschutzbeauftragten und der Leitung zu melden. Der Datenschutzbeauftragte trifft die Entscheidung, ob der Vorfall gemeldet werden muss. In diesem Fall ist innerhalb von 72 Stunden die jeweils zuständige Aufsichtsbehörde zu informieren
https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf,
(Datenschutz-Grundverordnung, Seite 96) und der Datenschutzvorfall zu dokumentieren. Bei Datenschutzanfragen ist der Datenschutzbeauftragte sofort einzubeziehen.

Der Datenschutzbeauftragte muss bei Vorfällen:

- die Ursache ermitteln und beseitigen
- die negativen Folgen eindämmen
- die Risiken neu bewerten
- ggf. betroffene Personen informieren
- ggf. Auskunft an die Aufsichtsbehörde erteilen
- ggf. die Stelle Öffentlichkeitsarbeit einbeziehen.

Regelungen zur Meldung an die Aufsichtsbehörde und Benachrichtigungen gegenüber betroffenen Personen finden sich in den Art. 33 und 34 der DSGVO.

Datenschutzanfragen können vom jeweiligen Landesdatenschutzbeauftragten gestellt werden und müssen innerhalb eines angemessenen Zeitraums bearbeitet werden.

Auch betroffene Personen können Auskunft verlangen (Art. 15 DSGVO). Daneben haben die betroffenen Personen ein Recht auf Löschung, Sperrung und Berichtigung (Art. 16 und 17 DSGVO). Alle Mitarbeiter werden in den Sensibilisierungsmaßnahmen und Schulungen darüber informiert. Die Ansprechpartner für Rückfragen sind jedem Mitarbeiter bekannt.

Es sollten Maßnahmen getroffen werden, dass es leicht ist, seine Rechte wahrzunehmen
https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf,
(Datenschutz-Grundverordnung, Seite 67) Anfragen sind ernst zu nehmen und zu dokumentieren:

- Wer erfragt,
- was,
- auf welcher Rechtsgrundlage?

Wenn begründete Zweifel an der Richtigkeit der Identität des Anfragenden vorliegen, sollten zusätzliche Informationen zur Identitätsfeststellung eingeholt werden. Jede Auskunft ist eine Übermittlung von personenbezogenen Daten und darf nur erteilt werden, wenn eine Rechtsgrundlage vorhanden ist (siehe 4).

Bei Unsicherheiten und Fragen ist intern Rücksprache zu halten, bevor eine Auskunft erteilt wird.

9 Kontinuierlicher Verbesserungsprozess

Ziel ist es, den Datenschutz schrittweise zu verbessern.

Der Datenschutzbeauftragte überprüft vor Ort die Wirksamkeit der getroffenen Maßnahmen. Auf diese Weise wird regelmäßig der Ist-Zustand erhoben und mit den gesetzlichen Anforderungen abgeglichen. Es können so Korrekturen erkannt werden, die erforderlich sind und daraufhin umgesetzt werden. Es fließen dabei ein:

- aufgetretene Vorfälle,
- interne Anfragen bei Schulungen,
- externe Anfragen,
- bewertete Risiken,
- sich verändernde Prozesse,
- neue Technik.

Die Geschäftsführung wird in den lebenden Prozess des Datenschutzes als Entscheider einbezogen.

Jeder Mitarbeiter kann Verbesserungsvorschläge an den Datenschutzbeauftragten übermitteln.

Die Datenschutzdokumente sollten regelmäßig durch den Datenschutzbeauftragten, mindestens jährlich, auf Aktualität überprüft und ggf. angepasst werden.

10 Abkürzungsverzeichnis

Abkürzung	**Bedeutung**
a. F.	Alte Fassung
AO	Abgabenordnung
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
d. h.	das heißt
DSGVO	Datenschutzgrundverordnung bzw. EU-Datenschutzgrundverordnung
EUTB	Ergänzende unabhängige Teilhabeberatung
GGmbH	Gemeinnützige Gesellschaft mit beschränkter Haftung
ggü.	gegenüber
HGB	Handelsgesetzbuch
KunstUrG	Kunsturhebergesetz
n. F.	Neue Fassung
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
u. a.	unter anderem
USB	
USV	Unterbrechungsfreie Stromversorgung
usw.	Und so weiter
z. B.	zum Beispiel
ZIP	Von englisch „Zipper“, Reißverschluss, ein Dateiformat, ein Dateikomprimierungssystem zum Zusammenfassen von Dateien, eine Art Containerdatei, kann mit Passwort versehen werden

11 Anhänge

11.1 Was Sie beachten müssen, wenn….

Ausfüllhilfe

Wenn Sie Ihr Dokument angepasst haben, löschen Sie bitte die Links mit den Hinweisen 1 bis X sowie diese Seite vollständig.

Hinweis 1

Tragen Sie den vollständigen Namen des Trägers Ihrer Beratungsstelle ein.

Hinweis 2

Tragen Sie den vollständigen Namen sowie die Adresse Ihrer Beratungsstelle ein.

Hinweis 3

In die nachfolgenden Zeilen alle Kontaktdaten der/ des betrieblichen Datenschutzbeauftragten angeben.