9.3.1 Datenschutzkonzept

Inhaltsverzeichnis

1 Einleitung

Dieses Datenschutzkonzept beschreibt sämtliche Maßnahmen, die der Caritasverband Gladbeck e.V. (im Folgenden Verband) zum Zwecke der Einhaltung der datenschutzrechtlichen Anforderungen und der nationalen und europäischen Vorschriften zum Datenschutz getroffen hat. Die hier genannten Anforderungen sind bei zukünftigen Maßnahmen und Projekten von allen Beschäftigten zu beachten. Die Aufgabe der Leitungskräfte ist es, deren Einhaltung sicherzustellen.
Dem Datenschutz kommt eine sehr hohe Bedeutung zu. Er ist gesetzlich vorgeschrieben und ist unserem Verband aus Gründen des Beschäftigten- und Kund*innenschutzes ein wichtiges Anliegen. Die Einhaltung ist auch insofern wichtig, als Verstöße gegen diese Vorschriften für unseren Verband zu Bußgeldern in existenzgefährdender Höhe führen können sowie Schadenersatzansprüche der Betroffenen zur Folge haben können. Fälle von Datenverlust können darüber hinaus einen erheblichen Imageschaden verursachen.
Es liegt in der Verantwortung aller Beschäftigten, durch Einhaltung dieses Datenschutzkonzeptes solche Schäden für unseren Verband zu vermeiden. Das Datenschutzmanagementsystem unseres Verbands ist in seinen wesentlichen Bestandteilen in diesem Datenschutzkonzept festgelegt. Ein Datenschutzmanagementsystem erschöpft sich nicht in einem einmaligen Aufbau, sondern ist ein kontinuierlicher Prozess. In diesem Zusammenhang hat sich der Plan-Do-Check-Act Zyklus (PDCA-Zyklus) bewährt und wird diesem Datenschutzkonzept zugrunde gelegt.

2 Geltungsbereich des Konzepts

Dieses Datenschutzkonzept regelt die datenschutzkonforme Informationsverarbeitung und die insoweit für den Verband bestehenden Verantwortlichkeiten. Die für die Verarbeitungen mit den eingesetzten Systemen verantwortlichen Leitungskräfte stellen sicher, dass die Beschäftigten im Sinne des Datenschutzrechts (=Mitarbeitende) über dieses Konzept informiert werden. Das gilt auch für temporär Beschäftigte. Der Datenschutzbeauftragte berät bei der Umsetzung des Konzepts und prüft dessen Einhaltung. Insoweit sind alle Adressaten dieses Datenschutzkonzepts dem Datenschutzbeauftragten auskunftspflichtig.

Dieses Datenschutzkonzept gilt für alle Dienste, Einrichtungen und Standorte des Verbandes.

3 Leitlinie zur Informationssicherheit und zum Datenschutz

Unser Verband bekennt sich zu den Anforderungen der Informationssicherheit und des Datenschutzes als wichtige Unternehmensziele. Zur Sicherstellung der sich daraus ergebenden Anforderungen hat der Verband dieses vorliegende Datenschutzkonzept erlassen. Daneben werden soweit erforderlich weitere Richtlinien im Bereich der Informationssicherheit und des Datenschutzes erlassen. Alle Beschäftigten haben die vorliegenden Regelungen zu beachten.

4 Datenschutzmanagementsystem

4.1 Einführung eines Datenschutzmanagementsystems

Im Gesetz über den kirchlichen Datenschutz (im Folgenden KDG) ist eine Vielzahl an Dokumentations-, Melde-, Nachweis- und Konsultationspflichten verankert. Zur Sicherstellung einer systematischen und dauerhaften Umsetzung dieser Vorgaben hält der Verband ein Datenschutzmanagementsystem (im Folgenden DSMS) vor. Dieses basiert auf einem kontinuierlichen Verbesserungsprozess, der darauf ausgerichtet ist, datenschutzrelevante Themen und Anforderungen im Verband zu implementieren. Es orientiert sich hierbei gedanklich an dem etablierten PDCA (Plan-Do-Check-Act)-Zyklus. Der PDCA-Zyklus gilt sowohl für die Einführung des Datenschutzmanagements als auch für die in diesem Rahmen getroffenen oder noch zu treffenden einzelnen Maßnahmen.
Ziel des PDCA-Zyklus ist es in diesem Zusammenhang, eine rechtswidrige Verarbeitung personenbezogener Daten zu verhindern. Seine Anwendung soll zugleich den im KDG festgelegten obligatorischen Dokumentations- und Rechenschaftspflichten genügen und den Verband in die Lage versetzen, jederzeit den Nachweis über die Einhaltung und Kontrolle der Pflicht zur rechtskonformen Verarbeitung in rechtlicher, technischer und organisatorischer Sicht führen zu können.

4.2 Inhalte des PDCA-Zyklus

Ein PDCA-Zyklus besteht aus vier Elementen:

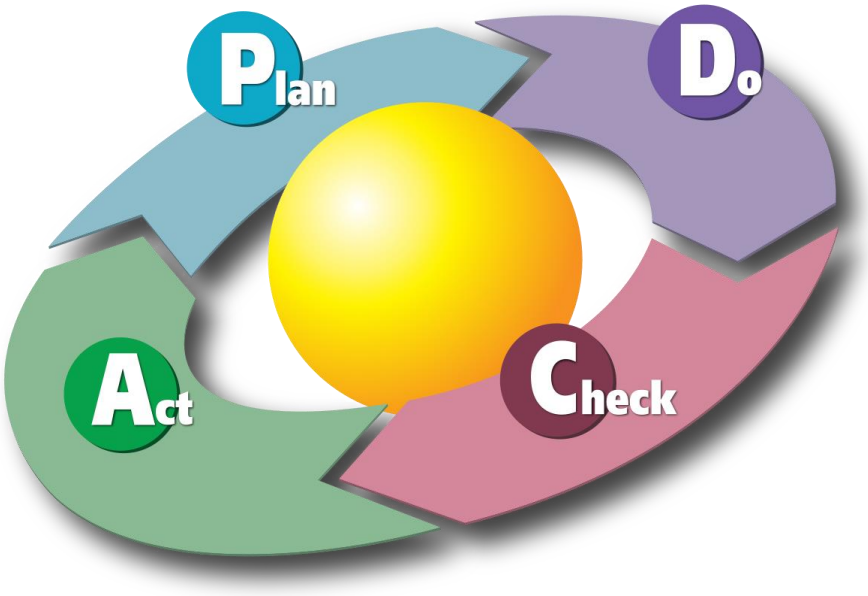

Diagramm von Karn G. Bulsuk (http://www.bulsuk.com)

Diese Elemente lassen sich in Bezug auf Datenschutz folgendermaßen konkretisieren:

Plan

Der jeweilige Prozess muss vor seiner eigentlichen Umsetzung geplant werden: „Plan“ umfasst das Erkennen von Verbesserungspotentialen (zum Beispiel durch Beschäftigte oder Leitungskräfte vor Ort), die Analyse sollte risikoorientiert erfolgen.

Do
Für die Umsetzung sind geeignete technische und organisatorische Maßnahmen zur Sicherstellung des Datenschutzes vorzusehen. Es ist der Nachweis der Verarbeitung in Übereinstimmung mit dem KDG (zumindest im Verzeichnis der Verarbeitungen) zu dokumentieren.

Check
Die getroffenen Maßnahmen sind hinsichtlich ihres Erfolges in Hinblick auf die Einhaltung des Datenschutzes zu überprüfen.

Act
Maßnahmen, bei denen im Rahmen der Erfolgskontrolle und Überwachung festgestellt wird, dass sie in datenschutzrechtlicher Hinsicht von den gesetzlichen Zielvorgaben abweichen, sind anzupassen. Die Verbesserung der Maßnahmen beginnt wiederum mit der Phase „Plan“.

4.3 Datenschutzevaluation / Datenschutzbericht

Der Datenschutzbeauftragte führt in jährlichen Abständen eine Datenschutzevaluation durch. Hierzu hat der Verband einen Fragenkatalog zu beantworten. Auf der Basis des Fragenkatalogs und der Erkenntnisse des Berichtsjahrs erstellt der Datenschutzbeauftragte als Ergebnis der Prüfung einen Jahresdatenschutzbericht.

5 Angaben zum Datenschutzbeauftragten

5.1 Bestellung des Datenschutzbeauftragten

Als betrieblicher Datenschutzbeauftragter ist Herr Michael Bock bestellt. Die Kontaktdaten des Datenschutzbeauftragten sind:
Daseco Consulting, RA Michael Bock, LL.M., Werkmeisterstraße 41, 47877 Willich, Telefon 02154 481575, Fax 02154 481576, Mobil 0170 2222242, E-Mail: mb@ra-bock.de

Die Benennung des Datenschutzbeauftragten ist dem Katholischen Datenschutzzentrum als zuständige Aufsichtsbehörde für den Datenschutz mitzuteilen.
Der Datenschutzbeauftragte ist in der Ausübung seiner Fachkunde frei.

5.2 Aufgaben des Datenschutzbeauftragten

Aufgabe des Datenschutzbeauftragten ist die Erfüllung der sich aus den Datenschutzgesetzen ergebenden Verpflichtungen. Im Einzelnen sind die Aufgaben:

- Fachkundige Beratung und Unterrichtung der Verantwortlichen bzw. Auftragsverarbeiter;
- Vertraut-Machen der konkret mit der Datenverarbeitung Beschäftigten mit den jeweiligen besonderen Erfordernissen des Datenschutzes;
- Beratung und Unterstützung der konkret mit der Datenverarbeitung Beschäftigten bei der Lösung von konkreten datenschutzrechtlichen Fragestellungen;

- Überwachung der Einhaltung des Datenschutzrechts. Hierzu ist der Datenschutzbeauftragte berechtigt, Kontrollen vor Ort durchzuführen und Einsicht in personenbezogene Daten zu nehmen;
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung;
- Achtung auf die Wahrung der Rechte der Betroffenen bei der Verarbeitung ihrer Daten; Fachkundige Unterstützung bei der Erstellung von datenschutzrelevanten betriebsinternen Verfahren, Anweisungen und Richtlinien (Datenschutz-Managementsystem);
- Ansprechperson für alle Beschäftigten ggf. auch unter Wahrung der Vertraulichkeit;
- Kooperation bei der Erfüllung der Aufgaben mit der Aufsichtsbehörde und Ansprechperson für die Aufsichtsbehörde in allen Fragen zur Verarbeitung von personenbezogenen Daten.

Der Datenschutzbeauftragte wird frühzeitig in alle Datenschutzfragen eingebunden und wird sowohl vom Vorstand als auch von den Beschäftigten bei der Erfüllung der o.g. Aufgaben unterstützt.

6 Datenschutzkoordination / Datenschutzmultiplikation

Als Ansprechperson für den Datenschutzbeauftragten ernennt der Verband eine Datenschutzkoordinatorin. Sie informiert den Datenschutzbeauftragten über vor Ort auftretende Datenschutzfragen, erhebt die Angaben über eingesetzte Verfahren und gibt die Meldung an den Datenschutzbeauftragten weiter.
Soweit es sich aufgrund organisatorischer Gegebenheiten als notwendig erweist, ernennt der Verband pro Dienst/Einrichtung/Standort weitere Datenschutzmultiplikator*innen.
Aus Gründen der Effektivität sollten Anfragen an den Datenschutzbeauftragten möglichst über die Datenschutzkoordinatorin oder die Datenschutzmultiplikator*innen des Verbandes erfolgen.

7 Erhebung/Verarbeitung von personenbezogenen Daten

Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen erfolgen. Hierbei sind auch die Voraussetzungen für die Erhebung und Verarbeitung besonderer personenbezogener Daten gemäß § 11 KDG zu beachten. Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen. Der Umgang mit personenbezogenen Daten muss durch Rechtsgrundlagen legitimiert sein.

8 Verwendung personenbezogener Daten zum Zwecke des Marketings

„Dialogmarketing ist eine Form des Direktmarketings, die im Gegensatz zu anderer unspezifischer Werbung, beispielsweise Außenwerbung, gezielt auf die Interessen der (potentiellen) Kund/innen zugeschnittene Produkte und Dienstleistungen anbietet und sich dabei wesentlich auf die Auswertung und Vertiefung bestehender und/oder vergangener Kundenbeziehungen stützt oder neue aufbaut.“ (https://de.wikipedia.org/wiki/Dialogmarketing, 17.04.2018) Bei der Verwendung personenbezogener

Daten im Rahmen des Dialogmarketings ist sicherzustellen, dass es eine Stelle im Verband gibt, die sämtliche Datenerhebungen und Verarbeitungen freigeben muss und hierfür verantwortlich ist. Bei der Erhebung der personenbezogenen Daten ist darauf zu achten, dass hierfür eine gültige Rechtsgrundlage vorhanden ist. Im Falle einer Einwilligung muss sichergestellt werden, dass die gesetzlichen Voraussetzungen für eine wirksame Einwilligung vorhanden sind und deren Vorliegen jederzeit nachgewiesen werden kann. Bei der Erhebung von personenbezogenen Daten ist ferner sicherzustellen, dass der Nutzer/die Nutzerin alle Informationen erhält, die datenschutzrechtlich vorgesehen sind. Die Verwendungszwecke sind bei der Datenerhebung im Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren.

9 Änderung von Zwecken der Verarbeitung personenbezogener Daten

Vor Einführung neuer Verarbeitungen ist die die Zulässigkeit bestimmende Zweckbestimmung der Daten durch den für die Anwendung Verantwortlichen schriftlich zu dokumentieren. Grundsätzlich ist eine Zweckänderung nur dann zulässig, wenn die Voraussetzungen des § 6 Abs. 2 und 4 KDG erfüllt sind. Die im Rahmen der Zweckänderung genutzten Abwägungskriterien sind einzeln zu prüfen. Die Prüfung ist darüber hinaus auch in einem ordnungsgemäßen Nachweis zu dokumentieren.

10 Weitergabe von personenbezogenen Daten

Falls andere Stellen Informationen über Betroffene anfordern, ist dies ohne Einwilligung der betroffenen Personen nur auf der Grundlage der §§ 9 und 10 KDG zulässig. Im Zweifel ist der Datenschutzbeauftragte zu kontaktieren.
Auskünfte an Polizeibehörden werden in Zweifelsfällen in Abstimmung mit dem Datenschutzbeauftragten erteilt. Bei wiederkehrenden, vergleichbaren Fällen ist eine Abstimmung nicht erneut erforderlich.
Sofern eine Herausgabe ohne Einwilligung der/des betroffenen Beschäftigten erfolgen soll, ist zumindest ein schriftliches Ersuchen der Polizeibehörde / der Staatsanwaltschaft erforderlich, wonach die Daten als Zeuge herauszugeben sind.

11 Grundsätze der Datenverarbeitung und Rechenschaftspflichten

Die Verarbeitung personenbezogener Daten ist laut § 6 KDG rechtmäßig, wenn eine der folgenden Voraussetzungen erfüllt ist:

- Das KDG oder eine andere kirchliche oder staatliche **Rechtsvorschrift** erlaubt sie oder ordnet sie an.
- Die betroffene Person hat ihre wirksame **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- Die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung **vorvertraglicher Maßnahmen** erforderlich, die auf Anfrage der betroffenen Person erfolgt;
- Die Verarbeitung ist zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;
- Die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen;

- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die **im kirchlichen Interesse** liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- Die Verarbeitung ist zur Wahrung der **berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um eine/n Minderjährige/n handelt (gilt nicht für die von öffentlich-rechtlich organisierten kirchlichen Stellen in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung).

Darüber hinaus müssen personenbezogene Daten laut § 7 KDG:

- auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („**Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**“);
- für **festgelegte**, eindeutige und legitime Zwecke erhoben werden; Personenbezogene Daten dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („**Zweckbindung**“);
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („**Datenminimierung**“);
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („**Richtigkeit**“);
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („**Speicherbegrenzung**“);
- in einer Weise verarbeitet werden, die eine **angemessene Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („**Integrität und Vertraulichkeit**“);

Den Verband treffen hinsichtlich der Einhaltung der oben genannten Punkte sogenannte „**Rechenschaftspflichten**“, d.h. er ist dazu verpflichtet, die hierzu im Einzelnen getroffenen Maßnahmen für jede Verarbeitungstätigkeit (zumindest im Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren.

12 Datenschutzorganisation

12.1 Organisation

Nach den verschiedenen datenschutzrechtlichen Vorschriften hat der Verband die Aufgabe, die Einhaltung der oben genannten datenschutzrechtlichen Maßnahmen und Anforderungen sicherzustellen. Als Ansprechperson für Fragen zum Datenschutz fungiert, sofern intern keine Datenschutzkoordinatorin benannt ist, der betriebliche Datenschutzbeauftragte des Verbandes. Er berät die für die Verarbeitung verantwortliche Person und überwacht die Einhaltung des Datenschutzes.

Alle Leitungskräfte sind verpflichtet, den Datenschutzbeauftragten bei Fragestellungen mit datenschutzrechtlicher Relevanz zur Beratung hinzuzuziehen.

12.2 Dokumentenablage

Die aktuelle Datenschutzdokumentation wird bei der Datenschutzkoordinatorin und beim Datenschutzbeauftragten geführt und gepflegt. Der Verband hat diese hierbei zu unterstützen und angefragte Informationen beizusteuern. Wichtige Formulare und Dokumente werden zusätzlich im Organisationshandbuch CVG vorgehalten, damit alle Beschäftigten darauf Zugriff haben.

12.3 Prüfung automatisierter Datenverarbeitung

Der Datenschutzbeauftragte prüft alle automatisierten Verarbeitungen, bei denen personenbezogene Daten verarbeitet werden. Damit diese Kontrolle möglich ist, ist ihm das Verzeichnis der Verarbeitungstätigkeiten zur Verfügung zu stellen. Die Verantwortung hierzu trifft im Zweifel die für die jeweilige Verarbeitungstätigkeit verantwortliche Leitungskraft.

12.4 Datenschutz-Folgenabschätzung

Sofern eine Form der Verarbeitung voraussichtlich eine hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, ist laut § 35 KDG durch den Verantwortlichen eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der personenbezogenen Daten durchzuführen. Bei der Durchführung der Datenschutz-Folgenabschätzung hat der Verantwortliche rechtzeitig den Rat des Datenschutzbeauftragten einzuholen. Eine Datenschutz-Folgenabschätzung ist zwingend erforderlich, wenn die Form des Verarbeitungsvorgangs auf der Liste der relevanten Verarbeitungsvorgänge der Aufsichtsbehörde enthalten ist, für die eine Datenschutz-Folgenabschätzung erwartet wird oder bei einer:

- systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
- umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten oder
- systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche.

Der Verantwortliche hat bei der Folgenabschätzung gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertretungen zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder kirchlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge einzuholen.
Wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, hat der Verband vor der Verarbeitung die Aufsichtsbehörde zu konsultieren. Die Durchführung einer Datenschutz-Folgenabschätzung erfolgt mithilfe des Formulars Datenschutz-Folgenabschätzung.

12.5 Verzeichnis aller Verarbeitungstätigkeiten (eigene Verarbeitungen)

Die im Verband existierenden Verarbeitungstätigkeiten, bei denen personenbezogene Daten verarbeitet werden, sind zu dokumentieren. Sie sind in der Liste der Verarbeitungstätigkeiten aufzuführen. Die jeweils aktuelle Liste der Verarbeitungstätigkeiten ist im Organisationshandbuch abgelegt und wird dem Datenschutzbeauftragten zu Kontrollzwecken zur Verfügung gestellt.

Die eigentliche Dokumentation der Verarbeitung erfolgt in einem Word-Formular. Das Formular Verarbeitungstätigkeiten – Verantwortlicher ist für alle in der Liste der Verarbeitungstätigkeiten erfassten Verarbeitungstätigkeiten von den jeweiligen Dienst- bzw. Einrichtungsleitungen auszufüllen und in jährlichem Abstand sowie bei Änderungen zu aktualisieren.
Für jedes Verfahren sind eine dokumentierte Schutzbedarfsfeststellung sowie eine Analyse bzgl. der für die betroffene Person möglichen Risiken zu erstellen. Die Risikoanalyse hat die Art, den Umfang, die Umstände und Zwecke der Verarbeitung sowie die Wahrscheinlichkeit des Eintritts einer solchen Gefahr zu berücksichtigten. Sie ist Bestandteil des Formulars Verarbeitungstätigkeiten – Verantwortlicher.

12.6 Verzeichnis aller Verarbeitungstätigkeiten (Verarbeitung für Auftraggeber)

Sofern der Verband als Auftragsverarbeiter Dienstleistungen übernimmt, in dessen Rahmen personenbezogene Daten verarbeitet werden oder ein Zugriff auf diese Daten ermöglicht wird (z.B. Fernwartung), besteht für jede Verarbeitungstätigkeit gegenüber den Auftraggebern die Verpflichtung, das Formular Verarbeitungstätigkeiten - Auftragsverarbeiter auszufüllen. Diese Dienstleistungen sind ferner in die Liste der Verarbeitungstätigkeiten mit aufzunehmen. In diesem Fall sind keine Angaben zum Zweck der Verarbeitung, zur Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogenen Daten und der Kategorien von Empfängern zu machen. Ebenfalls entfällt die Angabe der vorgesehenen Fristen für eine Löschung der personenbezogenen Daten und die umfangreiche Dokumentationspflicht. Aus diesem Grund gibt es hierfür ein eigenes Word Formular.

12.7 Auftragskontrolle, Vertragsschluss mit Auftragsverarbeitern

In allen Fällen, in denen personenbezogene Daten durch einen Dienstleister verarbeitet werden oder die Möglichkeit eines Zugriffs eines Dienstleisters auf solche Daten besteht (z.B. bei Wartungszugriffen), ist zu prüfen, ob Auftragsverarbeitung vorliegt. In Zweifelsfällen ist der Datenschutzbeauftragte zu informieren. Bei Auftragsverarbeitung hat der Verband als Auftraggeber vor einer Auftragserteilung eine Kontrolle durchzuführen und sich davon zu überzeugen, dass eine gesetzeskonforme, datenschutzgerechte Auftragsverarbeitung möglich ist. Daneben sind regelmäßige Auftragskontrollen durchzuführen und zu dokumentieren. Zu diesem Zweck müssen alle Auftragsverarbeiter regelmäßig einen Fragebogen zur Auftragskontrolle hinsichtlich der getroffenen technischen und organisatorischen Maßnahmen ausfüllen oder den Nachweis auf anderem Wege erbringen (z.B. durch Bescheinigungen, Gutachten, Duldung von Kontrollen vor Ort, etc.).

Besondere Bedeutung kommt auch im Rahmen der vorgelagerten Vertragsverhandlung der datenschutzgerechten Vertragsgestaltung zu, da nach dem Gesetzeswortlaut gewisse Mindestinhalte schriftlich vereinbart werden müssen.
Sollen externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. einzelner Verarbeitungsschritte (z.B. Erhebung, Löschung/Entsorgung) bzw. mit Tätigkeiten (z.B. Wartung, Reparatur) beauftragt werden, bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten bekommen, so ist der Datenschutzbeauftragte vor der Beauftragung unter Vorlage des den Anforderungen des Datenschutzes genügenden Vertragsentwurfs und der Kriterien der erfolgten bzw. nachfolgend vorgesehenen Auftragskontrolle zu informieren. Die Checkliste Abschluss einer Auftragsverarbeitung und der Fragebogen zur Auftragskontrolle stehen im Organisationshandbuch zur Verfügung. Die aktuelle Liste der Auftragsverarbeiter (zum Zweck der Ergänzung neuer Auftragsverarbeiter) wird von der Datenschutzkoordinatorin geführt.
Die Dienst- bzw. Einrichtungsleitungen und die für den Einkauf zuständigen Beschäftigten sind verpflichtet sicherzustellen, dass sämtliche Auftragsverarbeiter die o.g. Kriterien erfüllen und in die Liste der Auftragsverarbeiter aufgenommen werden. Der Datenschutzbeauftragte erhält eine Kopie der unterschriebenen Verträge.

12.8 Ausübung von Betroffenenrechten

Das Datenschutzrecht sieht verschiedene Betroffenenrechte vor. Im Wesentlichen sind hier die Rechte auf Auskunft, Berichtigung, Löschung oder das Recht auf Einschränkung der Verarbeitung (Sperrung) sowie auf "Vergessenwerden" zu nennen.
Ein zentraler Bestandteil ist die umfassende Information der betroffenen Person über die Datenverarbeitung und die Wahrnehmung ihrer Rechte.
Die insgesamt aus Sicht des Betroffenendatenschutzes vom Verband zu treffenden Maßnahmen sind:

- Organisatorische Regelungen für Beschäftigte über
  - Informations- und Mitteilungspflichten bei Anfragen durch Betroffene
  - Prüfung der Rechtmäßigkeit der Datenverarbeitung
  - Zweckbindung und Datenminimierung
  - Datenschutzverletzungen und die damit verbundenen Meldepflichten
- Dokumentation der Datenverarbeitung
  - Verzeichnis der Verarbeitungstätigkeiten
  - Datenschutzerklärung über Umfang, Zweck und Dauer der Datenverarbeitung
- Strukturierte Datenhaltung zum vollständigen Auffinden der Daten der Betroffenen
- Datenabschottung und Datentrennung
- Festlegung von Löschfristen
- Implementierung von Lösch- und Berichtigungsfunktionen
- Datenexportierbarkeit für die Datenübertragbarkeit

Betroffenenrechte können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.
Auf Betroffenenanfragen ist grundsätzlich innerhalb eines Monats zu reagieren. Die Verletzung der Frist stellt einen bußgeldbewehrten Verstoß dar. Besondere Beachtung verdienen insbesondere die folgenden Punkte:

12.9 Einwilligung, Transparenz- und Informationspflicht

Vor Beginn der Datenverarbeitung muss die betroffene Person entweder einwilligen oder über die rechtliche Grundlage, ihre Rechte und weitere Punkte informiert werden. Einwilligungen und Informationen sind zu prüfen auf:

- Rechtskonforme Gestaltung der Einwilligung, zuverlässige Dokumentation und Berücksichtigung in nachfolgenden Verarbeitungsprozessen
- Information der betroffenen Personen (z.B. Kund*innen, Beschäftigte) über die Rechtsgrundlage
- Information der betroffenen Personen (z.B. Kund*innen, Beschäftigte) über Betroffenenrechte
- Information über weitere Pflichtangaben.

Vollständige und inhaltlich korrekte Einwilligungen und Informationen für Betroffene sind von den zuständigen Dienst- bzw. Einrichtungsleitungen anhand der Formulare Einwilligung und Datenschutzinformation zu erstellen.

12.10 Datenselbstauskünfte von Betroffenen, Recht auf Löschung, Korrektur, Sperrung

Macht eine betroffene Person von ihrem Auskunftsrecht oder ihrem Korrektur- oder Widerspruchsrecht Gebrauch, ist der Datenschutzbeauftragte einzubeziehen, sofern es sich nicht um wiederkehrende Fragestellungen handelt, die bereits grundsätzlich mit ihm abgestimmt wurden. Datenschutzanfragen werden durch die zuständige Abteilungsleitung beantwortet. Es ist sicherzustellen, dass der betroffenen Person ihre Daten auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden können. Welcher Standard diesen Anforderungen genügt, ist im Vorfeld einvernehmlich durch den Datenschutzbeauftragten und den Fachdienst ITTK festzulegen.
Für das Einsichtsrecht in die Personalakte durch Beschäftigte ist die Personalabteilung zuständig. Zur Sicherstellung von Auskunftsansprüchen hat die Personalabteilung Vorsorge dafür zu treffen, dass die Auskunft vollständig erteilt werden kann. Dabei sind u.U. auch Aufzeichnungen auf Papierunterlagen mit einzubeziehen, wenn die betroffene Person ihren Anspruch in dieser Hinsicht konkretisiert oder das Vorhandensein solcher Unterlagen offensichtlich ist.

13 Beschäftigtendatenschutz

13.1 Verpflichtung der Beschäftigten auf den Datenschutz

Der Verband ist verpflichtet, die Beschäftigten über den Datenschutz zu belehren. Die Mitarbeitenden des Fachdienstes ITTK werden darüber hinaus auf das Fernmeldegeheimnis nach § 88 TKG verpflichtet. In Einzelfällen könnte eine Verpflichtung auf das Bank- oder Sozialgeheimnis erforderlich sein. Die jeweilige Verpflichtungserklärung wird Bestandteil der Personalakte. Der/Die Beschäftigte erhält eine Kopie der Erklärung.

13.2 Information der Beschäftigten mit Tätigkeitsbeginn

Alle Beschäftigten sollen innerhalb von 14 Tagen nach Beschäftigungsbeginn eine schriftliche oder mündliche Unterweisung zum Datenschutz erhalten und die Prozessbeschreibung Datenschutz (noch nicht in Kraft) sowie die Dienstanweisung Datenschutz zur Kenntnis nehmen.

13.3 Informationen zum Datenschutz für die Beschäftigten

Für die Beschäftigten werden im Organisationshandbuch CVG alle wesentlichen Informationen zum Datenschutz zur Verfügung gestellt.

14 Information bei Sicherheitsvorfällen und bei Datenverlust

Im Falle eines Datenverlustes, eines möglichen Datenverlustes oder einer unrechtmäßigen Verarbeitung von personenbezogenen Daten, also **bei jeglicher Verletzung des Schutzes personenbezogener Daten,** kann es je nach Einzelfall erforderlich sein, **innerhalb von 72 Stunden** die Aufsichtsbehörde und ggf. sobald wie möglich die Betroffenen zu informieren. Eine Missachtung dieser Verpflichtung kann mit hohen Bußgeldern für den Verband oder verantwortliche Beschäftigte geahndet werden. Zur Einhaltung der gesetzlichen Rahmenbedingungen und Vermeidung von Bußgeldern ist das folgende Verfahren zwingend einzuhalten:

- Der Vorstand ist unverzüglich mit dem Formular Meldung einer Datenpanne zu informieren.
- Er prüft den Sachverhalt ggf. unter Hinzuziehung des Datenschutzbeauftragten und eines rechtlichen Beistandes.
- In den Fällen, in denen eine Meldepflicht nicht ausgeschlossen werden kann, informiert der Vorstand unverzüglich die Aufsichtsbehörde.
- Soweit der Verband gegenüber einem anderen Unternehmen als Auftragsverarbeiter tätig ist und ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich mit dem Formular Meldung Datenpanne Auftraggeber (noch nicht in Kraft).

15 Informationssicherheit

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 des KDG zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Die Maßnahmen des Verbandes sind in 9.3.4.5 Technische und organisatorische Maßnahmen aufgeführt.

15.1 Anforderungen zur Informationssicherheit

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),
3. zu gewährleisten, 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 (**Zugriffskontrolle**),
4. zu gewährleisten, 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 (**Weitergabekontrolle**),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Bei der Umsetzung seiner technischen und organisatorischen Maßnahmen hat der für die Verarbeitung Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

- Die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Nach den datenschutzrechtlichen Vorschriften hat der Verband unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen einzusetzen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß den Datenschutzvorschriften und diesem Datenschutzkonzept erfolgt.

Daraus ergibt sich für den Verband die Verpflichtung, für seine Verarbeitungstätigkeiten, bei denen personenbezogene Daten verarbeitet werden, in Hinblick auf die Datensicherheit die folgenden Maßnahmen durchzuführen:

1. Feststellen des Schutzbedarfes.
2. Risikoanalyse
3. Treffen und Umsetzen der jeweiligen Maßnahmen zur Risikovermeidung bzw. -verringerung.
4. Führen von Dokumentationen und Nachweisen.
5. Regelmäßige Überprüfung der getroffenen Maßnahmen im Bereich der Datensicherheit.

Soweit möglich wird sich der Verband hierbei an dem gängigen Standard im Bereich der Informationssicherheit orientieren.

15.2 Anforderungen Privacy by design und Privacy bei Default

Soweit eigene Software entwickelt wird oder neue Software durch Softwareentwickler / -anbieter bezogen wird, ist darauf zu achten, dass die Grundsätze der Datensparsamkeit berücksichtigt werden. Durch Voreinstellungen ist sicherzustellen, dass personenbezogene Daten grundsätzlich nur für den jeweiligen Verarbeitungszweck genutzt werden, für den sie erforderlich sind. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung und die Speicherdauer und deren Zugänglichkeit. Für die Freigabe personenbezogener Daten sind Freigabeverfahren zu implementieren. Ggf. sind weitere Maßnahmen zu ergreifen, wie z.B. Pseudonymisierung, Anonymisierung, Datenminimierung, Sperren von Schnittstellen und Vorgeben von Löschfristen.
Falls mit der Beschaffung ein neues Verfahren der Verarbeitung personenbezogener Daten eingeführt werden soll, ist der Datenschutzbeauftragte rechtzeitig vorab von der zuständigen Dienst- bzw. Einrichtungsleitung zu informieren. Die Beschaffung erfolgt erst nach Stellungnahme des Datenschutzbeauftragten. Der Datenschutzbeauftragte berät dahingehend, ob die Durchführung einer Datenschutz-Folgenabschätzung erforderlich ist. Die Durchführung einer Datenschutz-Folgenabschätzung erfolgt mithilfe des Formulars Datenschutz-Folgenabschätzung.

16 Mitgeltende Dokumente

- 9.3.3.1 Gesetz über den kirchlichen Datenschutz (KDG)
- 9.3.2 Prozessbeschreibung Datenschutz (noch nicht in Kraft)
- 9.3.4.1 Dienstanweisung Datenschutz (noch nicht in Kraft)
- 9.3.5.1 Liste der Verarbeitungstätigkeiten
- 9.3.5.3 Liste der Auftragsverarbeiter
- 9.3.6.8 Formular Datenschutz-Folgenabschätzung (noch nicht in Kraft)

- 9.3.4.4 Richtlinie Mindestanforderungen an EDV-Kennwörter
- 9.3.4.2 Datenträgerentsorgung
- 9.3.6.1 Formular Verarbeitungstätigkeiten – Verantwortlicher
- 9.3.6.2 Formular Verarbeitungstätigkeiten – Auftragsverarbeiter (noch nicht in Kraft)
- 9.3.6.9 Checkliste Abschluss einer Auftragsverarbeitung
- 9.3.6.10 Fragebogen zur Auftragskontrolle von Auftragsverarbeitern (noch nicht in Kraft)
- 9.3.6.3 Formular Einwilligungserklärung
- 9.3.6.6 Formular Datenschutzinformation einfach
- 9.3.6.7 Formular Datenschutzinformation mehrfach
- 9.3.6.11 Formular Meldung einer Datenpanne (noch nicht in Kraft)
- 9.3.6.12 Formular Meldung einer Datenpanne – Auftraggeber (noch nicht in Kraft)
- 9.3.4.3 Verpflichtungserklärung

17 Inkrafttreten

Dies Dokument tritt mit seiner Freigabe und Veröffentlichung im Organisationshandbuch in Kraft und ist damit für sämtliche Beschäftigte des Verbandes verbindlich.