Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO)

in der Fassung des Beschlusses der Vollversammlung des
Verbandes der Diözesen Deutschlands vom 19. November 2018,
geändert durch Beschluss der Vollversammlung des
Verbandes der Diözesen Deutschlands vom 24. November 2025

Aufgrund des § 56 des Gesetzes über den Kirchlichen Datenschutz (KDG) vom 20. März 2018, veröffentlicht im Amtsblatt des Bistums Erfurt Nr. 3/2018 vom 20. März 2018, wird die folgende Durchführungsverordnung zum KDG (KDG-DVO) erlassen:

Inhaltsübersicht

Kapitel 4
Maßnahmen des Verantwortlichen und des oder der Mitarbeitenden

Kapitel 5
Besondere Gefahrenlagen

Kapitel 6
Übergangs- und Schlussbestimmungen

Kapitel 1
Verarbeitungstätigkeiten

§ 1
Verzeichnis von Verarbeitungstätigkeiten

(1) Das vom Verantwortlichen gemäß § 31 Absatz 1 bis Absatz 3 KDG zu führende Verzeichnis von Verarbeitungstätigkeiten ist dem oder der betrieblichen Datenschutzbeauftragten, sofern ein solcher oder eine solche benannt wurde, vor Beginn der Verarbeitung von personenbezogenen Daten und auf entsprechende Anfrage der Datenschutzaufsicht auch dieser unverzüglich zur Verfügung zu stellen.

(2) Sofern die zuständige Datenschutzaufsicht ein Muster für ein Verzeichnis von Verarbeitungstätigkeiten gemäß § 31 KDG zur Verfügung stellt, bildet dieses grundsätzlich den Mindeststandard.

(3) [1]Das Verzeichnis ist bei jeder Veränderung eines Verfahrens zu aktualisieren. [2]Im Übrigen ist es in regelmäßigen Abständen von höchstens zwei Jahren einer Überprüfung durch den Verantwortlichen zu unterziehen und bei Bedarf zu aktualisieren. [3]Die Überprüfung sowie die Aktualisierung sind in geeigneter Weise zu dokumentieren.

Kapitel 2

Datengeheimnis

§ 2
Belehrung und Verpflichtung auf das Datengeheimnis, Schulung

(1) Zu den bei der Verarbeitung personenbezogener Daten tätigen Personen im Sinne des § 5 KDG gehören die in den Stellen gemäß § 3 Absatz 1 KDG Beschäftigten im Sinne des § 4 Ziffer 24. KDG sowie die dort ehrenamtlich tätigen Personen (Mitarbeitende im Sinne dieser Durchführungsverordnung, im Folgenden: Mitarbeitende).

(2) [1]Durch geeignete Maßnahmen sind die Mitarbeitenden mit den Vorschriften des KDG sowie den anderen für ihre Tätigkeit geltenden Datenschutzvorschriften vertraut zu machen. [2]Dies geschieht im Wesentlichen durch Hinweis auf die für den Aufgabenbereich der Person wesentlichen Grundsätze und Erfordernisse und im Übrigen durch Bekanntgabe der entsprechenden Regelungstexte in der jeweils gültigen Fassung. [3]Das KDG und diese Durchführungsverordnung sowie die sonstigen Datenschutzvorschriften werden zur Einsichtnahme und etwaigen Ausleihe bereitgehalten oder elektronisch zur Verfügung gestellt; dies ist den Mitarbeitenden in geeigneter Weise mitzuteilen.

(3) Ferner sind die Mitarbeitenden zu belehren über

a) die Verpflichtung zur Beachtung der in Absatz 2 genannten Vorschriften bei der Verarbeitung personenbezogener Daten,
b) mögliche rechtliche Folgen eines Verstoßes gegen das KDG und andere für ihre Tätigkeit geltende Datenschutzvorschriften,
c) das Fortbestehen des Datengeheimnisses nach Beendigung der Tätigkeit bei der Datenverarbeitung.

(4) Bei einer wesentlichen Änderung des KDG oder anderer für die Tätigkeit der Mitarbeitenden geltender Datenschutzvorschriften sowie bei Aufnahme einer neuen Tätigkeit durch den Mitarbeitenden oder die Mitarbeitende hat insoweit eine erneute Belehrung zu erfolgen.

(5) [1]Die Mitarbeitenden haben in nachweisbar dokumentierter Form eine Verpflichtungserklärung gemäß § 3 abzugeben. [2]Diese Verpflichtungserklärung wird zu der Personalakte bzw. den Unterlagen des oder der jeweiligen Mitarbeitenden genommen. [3]Dieser oder diese erhält eine Ausfertigung der Erklärung.

(6) Die Verpflichtung auf das Datengeheimnis gemäß § 5 KDG erfolgt durch den Verantwortlichen oder einen von ihm Beauftragten.

(7) Die Mitarbeitenden sind regelmäßig zu schulen.

§ 3
Inhalt der Verpflichtungserklärung

(1) Die gemäß § 2 Absatz 5 nachweisbar zu dokumentierende Verpflichtungserklärung des oder der Mitarbeitenden gemäß § 5 Satz 2 KDG hat zum Inhalt

a) Angaben zur Identifizierung des oder der Mitarbeitenden (Vorname, Zuname, Beschäftigungsdienststelle, Personalnummer sowie, sofern Personalnummer nicht vorhanden, Geburtsdatum und Anschrift),
b) die Bestätigung, dass der oder die Mitarbeitende auf die für die Ausübung seiner oder ihrer Tätigkeit spezifisch geltenden Bestimmungen und im Übrigen auf die allgemeinen datenschutzrechtlichen Regelungen in den jeweils geltenden Fassungen sowie auf die Möglichkeit der Einsichtnahme und Ausleihe dieser Texte hingewiesen wurde,
c) die Verpflichtung des oder der Mitarbeitenden, das KDG und andere für seine Tätigkeit geltende Datenschutzvorschriften in den jeweils geltenden Fassungen sorgfältig einzuhalten,
d) die Bestätigung, dass der oder die Mitarbeitende über rechtliche Folgen eines Verstoßes gegen das KDG sowie gegen sonstige für die Ausübung seiner oder ihrer Tätigkeit spezifisch geltende Bestimmungen belehrt wurde.

(2) Die Verpflichtungserklärung ist von dem oder der Mitarbeitenden unter Angabe des Ortes und des Datums der Unterschriftsleistung zu unterzeichnen oder auf eine andere dem Verfahren angemessene Weise zu signieren.

(3) Sofern die zuständige Datenschutzaufsicht ein Muster einer Verpflichtungserklärung zur Verfügung stellt, bildet dieses den Mindeststandard.

Kapitel 3
Technische und organisatorische Maßnahmen

Abschnitt 1
Grundsätze und Maßnahmen

§ 4
Begriffsbestimmungen
(IT-Systeme, Lesbarkeit)

(1) IT-Systeme im Sinne dieser Durchführungsverordnung sind sämtliche technischen Einrichtungen, mittels derer personenbezogene Daten automatisiert verarbeitet werden.

(2) IT-Systeme sind insbesondere

a) hardwarebasierte IT-Komponenten (elektronische Geräte wie Server, Arbeitsplatzrechner, mobile Endgeräte, eingebettete Systeme (z.B. IoT) oder vergleichbare technische Komponenten, die einzeln oder im Verbund betrieben werden können),
b) Softwarelösungen (lokal installierte oder netzwerkgestützte Programme und Anwendungen einschließlich betriebssystemnaher Software und Anwendungssoftware, die unmittelbar oder mittelbar an der Verarbeitung personenbezogener Daten beteiligt sind),
c) cloudbasierte Systeme und Dienste (Bereitstellungsformen wie Software as a Service (SaaS), Platform as a Service (PaaS) oder Infrastructure as a Service (IaaS), die über netzwerkbasierte Umgebungen (insbesondere Internet oder Intranet) zugänglich sind und zur Datenverarbeitung eingesetzt werden).

(3) Unter Lesbarkeit im Sinne dieser Durchführungsverordnung ist die Möglichkeit zur vollständigen oder teilweisen Wiedergabe des Informationsgehalts von personenbezogenen Daten zu verstehen.

§ 5
Grundsätze der Verarbeitung

(1) Der Verantwortliche hat sicher zu stellen, dass bei der Verarbeitung personenbezogener Daten durch innerbetriebliche Organisation und mittels technischer und organisatorischer Maßnahmen die Einhaltung des Datenschutzes gewährleistet wird.

(2) Die Verarbeitung personenbezogener Daten auf IT-Systemen darf erst erfolgen, wenn der Verantwortliche und der Auftragsverarbeiter die nach dem KDG und dieser Durchführungsverordnung erforderlichen technischen und organisatorischen Maßnahmen zum Schutz dieser Daten getroffen haben.

§ 6
Technische und organisatorische Maßnahmen

(1) Je nach der Art der zu schützenden personenbezogenen Daten sind unter Berücksichtigung von §§ 26 und 27 KDG angemessene technische und organisatorische Maßnahmen zu treffen, die geeignet sind,

a) zu verhindern, dass unberechtigt Rückschlüsse auf eine bestimmte Person gezogen werden können (z.B. durch Pseudonymisierung oder Anonymisierung personenbezogener Daten),
b) einen wirksamen Schutz gegen eine unberechtigte Verarbeitung personenbezogener Daten insbesondere während ihres Übertragungsvorgangs herzustellen (z. B. durch Verschlüsselung mit geeigneten Verschlüsselungsverfahren; das Verschlüsselungsverfahren ist dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen auszuwählen),
c) die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste zum Schutz vor unberechtigter Verarbeitung auf Dauer zu gewährleisten und dadurch Verletzungen des Schutzes personenbezogener Daten in angemessenem Umfang vorzubeugen,
d) im Fall eines physischen oder technischen Zwischenfalls die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen rasch wiederherzustellen (Wiederherstellung).

(2) Im Einzelnen sind für die Verarbeitung personenbezogener Daten in elektronischer Form unabhängig vom Ort der Verarbeitungstätigkeit insbesondere folgende Maßnahmen zu treffen:

a) Unbefugten ist der Zutritt zu IT-Systemen im Sinne des § 4 Absatz 2 Nr. 1, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zutrittskontrolle).
b) [1]Es ist zu verhindern, dass IT-Systeme und Benutzerzugänge von Unbefugten genutzt werden können (Zugangskontrolle). [2]Zum Schutz personenbezogener Daten und zur Vermeidung von Identitätsdiebstahl sind geeignete technische und organisatorische Maßnahmen nach dem jeweiligen Stand der Technik zu ergreifen.

[3]Dies gilt insbesondere für Datenverarbeitungen außerhalb eines geschlossenen und gesicherten Netzwerks.

c) Die zur Benutzung eines IT- Systems Berechtigten dürfen ausschließlich auf die ihrer Zuständigkeit unterliegenden personenbezogenen Daten zugreifen können; personenbezogene Daten dürfen nicht unbefugt gelesen, kopiert, verändert oder entfernt werden (Zugriffskontrolle).

d) Personenbezogene Daten sind auch während ihrer elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern gegen unbefugtes Auslesen, Kopieren, Verändern oder Entfernen durch geeignete Maßnahmen zu schützen.

e) [1]Es muss überprüft und festgestellt werden können, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung erfolgt (Weitergabekontrolle). [2]Werden personenbezogene Daten außerhalb der vorgesehenen Datenübertragung weitergegeben, ist dies zu protokollieren.

f) [1]Es ist grundsätzlich sicher zu stellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in IT-Systemen verarbeitet worden sind (Eingabekontrolle). [2]Die Eingabekontrolle umfasst unbeschadet der gesetzlichen Aufbewahrungsfristen mindestens einen Zeitraum von sechs Monaten.

g) Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden (Auftragskontrolle).

h) Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).

i) Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden (Trennungsgebot).

j) Im Netzwerk- und im Einzelplatzbetrieb ist eine abgestufte Rechteverwaltung erforderlich. Anwender- und Administrationsrechte sind zu trennen.

k) Bei der Auswahl von IT-Systemen, insbesondere von Softwarelösungen, ist dem Grundsatz der Datenminimierung angemessen Rechnung zu tragen.

(3) Absatz 2 gilt entsprechend für die Verarbeitung personenbezogener Daten in nicht automatisierter Form.

§ 7
Überprüfung

(1) [1]Zur Gewährleistung der Sicherheit der Verarbeitung sind die getroffenen technischen und organisatorischen Maßnahmen durch den Verantwortlichen regelmäßig, mindestens jedoch im Abstand von jeweils zwei Jahren, auf ihre Wirksamkeit zu überprüfen. [2]Zu diesem Zweck ist ein für die jeweilige kirchliche Stelle geeignetes und angemessenes Verfahren zu entwickeln, welches eine verlässliche Bewertung des Ist-Zustandes und eine zweckmäßige Anpassung an den aktuellen Stand der Technik erlaubt.

(2) [1]Insbesondere die Vorlage eines anerkannten Zertifikats gemäß § 26 Absatz 4 KDG durch den Verantwortlichen, welches sich an Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) orientiert, ist als Nachweis zulässig. [2]Abweichend von Satz 1 kann auch eine Orientierung an anderen Regelungen erfolgen, die einen vergleichbaren Schutzstandard gewährleisten (insbesondere ISO/IEC 27001).

(3) Die Überprüfung nach Absatz 1 ist zu dokumentieren.

(4) Für den Fall der Auftragsverarbeitung gilt § 15 Absatz 5.

§ 8
Verarbeitung von Meldedaten in kirchlichen Rechenzentren

(1) Werden personenbezogene Daten aus den Melderegistern der kommunalen Meldebehörden in kirchlichen Rechenzentren verarbeitet, so orientieren sich die von diesen zu treffenden Schutzmaßnahmen an den jeweils geltenden BSI-IT-Grundschutzkatalogen oder vergleichbaren Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Abweichend von Satz 1 kann auch eine Orientierung an anderen Regelungen erfolgen, die einen vergleichbaren Schutzstandard gewährleisten (insbesondere ISO 27001 auf Basis IT-Grundschutz).

(2) Rechenzentren im Sinne dieser Durchführungsverordnung sind die für den Betrieb von größeren, zentral in mehreren Dienststellen eingesetzten Informations- und Kommunikationssystemen erforderlichen Einrichtungen.

Abschnitt 2
Schutzbedarf und Risikoanalyse

§ 9
Einordnung in Datenschutzklassen und Datenschutzniveau

(1) Unter Berücksichtigung der Art der zu verarbeitenden personenbezogenen Daten und des Ausmaßes der möglichen Gefährdung personenbezogener Daten hat eine Einordnung in eine der in §§ 11 bis 13 genannten drei Datenschutzklassen zu erfolgen.

(2) Bei der Einordnung personenbezogener Daten in eine Datenschutzklasse sind auch der Zusammenhang mit anderen gespeicherten Daten, der Zweck ihrer Verarbeitung und das anzunehmende Interesse an einer missbräuchlichen Verwendung der Daten zu berücksichtigen.

(3) [1]Die Einordnung erfolgt durch den Verantwortlichen; sie soll in der Regel bei Erstellung des Verzeichnisses von Verarbeitungstätigkeiten vorgenommen werden. [2]Der oder die betriebliche Datenschutzbeauftragte soll angehört werden.

(4) [1]In begründeten Einzelfällen kann der Verantwortliche eine abweichende Einordnung vornehmen. [2]Die Gründe sind zu dokumentieren. [3]Erfolgt eine Einordnung in eine niedrigere Datenschutzklasse, ist zuvor der oder die betriebliche Datenschutzbeauftragte anzuhören.

(5) Erfolgt keine Einordnung, gilt automatisch die Datenschutzklasse III, sofern nicht die Voraussetzungen des § 14 vorliegen.

(6) Die Einordnung in eine der nachfolgend genannten Datenschutzklassen erfordert die Einhaltung des dieser Datenschutzklasse entsprechenden Schutzniveaus und die Einhaltung der dort beschriebenen Mindestmaßnahmen.

(7) Erfolgt die Verarbeitung durch einen Auftragsverarbeiter, ist der Verantwortliche verpflichtet, sich in geeigneter Weise, insbesondere durch persönliche Überprüfung oder

Vorlage von Nachweisen, von dem Bestehen des der jeweiligen Datenschutzklasse entsprechenden Schutzniveaus zu überzeugen.

§ 10
Risikoanalyse

(1) Die den individuellen Gegebenheiten entspringenden Risiken sind vom Verantwortlichen anhand einer Risikoanalyse festzustellen.

(2) [1]Für eine Analyse der möglichen Risiken für die Rechte und Freiheiten natürlicher Personen, die mit der Verarbeitung personenbezogener Daten verbunden sind, sind objektive Kriterien zu entwickeln und anzuwenden. [2]Hierzu zählen insbesondere die Eintrittswahrscheinlichkeit und die Schwere eines Schadens für die betroffene Person. [3]Zu berücksichtigen sind auch Risiken, die durch – auch unbeabsichtigte oder unrechtmäßige – Vernichtung, durch Verlust, Veränderung, unbefugte Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten entstehen.

(3) Die identifizierten Risiken sind durch entsprechende Maßnahmen im Einklang mit § 6 zu behandeln.

§ 11
Datenschutzklasse I und Schutzniveau I

(1) Der Datenschutzklasse I unterfallen personenbezogene Daten, deren missbräuchliche Verarbeitung keine besonders schwerwiegende Beeinträchtigung des Betroffenen erwarten lässt. Hierzu gehören insbesondere Namens- und Adressangaben ohne Sperrvermerke sowie Berufs-, Branchen- oder Geschäftsbezeichnungen.

(2) Zum Schutz der in die Datenschutzklasse I einzuordnenden Daten ist ein Schutzniveau I zu definieren. Dieses setzt voraus, dass mindestens folgende Voraussetzungen gegeben sind:

a) Das IT-System, auf dem die schützenswerten personenbezogenen Daten abgelegt sind, ist nicht frei zugänglich; es befindet sich z.B. in einem abschließbaren Gebäude oder unter ständiger Aufsicht.
b) [1]Die Anmeldung am IT-System ist nur nach Eingabe eines geeigneten benutzerdefinierten Passwortes oder unter Verwendung eines anderen, dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechenden Authentifizierungsverfahrens zulässig. [2]In sicherheitskritischen Bereichen oder bei Zugriffen außerhalb gesicherter Netze ist insbesondere der Einsatz von Mehr-Faktor-Authentifizierungsverfahren (z. B. Kombination aus Passwort und Einmalcode, Hardware-Token oder biometrischen Verfahren) vorzusehen.
c) Sicherungskopien von Daten sind nach aktuellem Stand der Technik mit geeigneten Maßnahmen vor unbefugtem Zugriff zu schützen.
d) Vor der Weitergabe eines IT-Systems, insbesondere eines Datenträgers für einen anderen Einsatzzweck sind die auf ihm befindlichen Daten so zu löschen, dass ihre Lesbarkeit und ihre Wiederherstellung ausgeschlossen sind.
e) Nicht öffentlich verfügbare Daten werden nur dann weitergegeben, wenn sie durch geeignete Schutzmaßnahmen geschützt sind. Die Art und Weise des Schutzes ist vor Ort zu definieren.

§ 12
Datenschutzklasse II und Schutzniveau II

(1) Der Datenschutzklasse II unterfallen personenbezogene Daten, deren missbräuchliche Verarbeitung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann. Hierzu gehören z.B. Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und Jubiläumsdaten.

(2) Zum Schutz der in die Datenschutzklasse II einzuordnenden Daten ist ein Schutzniveau II zu definieren. Dieses setzt voraus, dass neben dem Schutzniveau I mindestens folgende Voraussetzungen gegeben sind:

a) [1]Die Anmeldung am IT-System ist nur nach Eingabe eines geeigneten benutzerdefinierten Passwortes zulässig, das ausreichend komplex gewählt werden muss und dessen Erneuerung nach dem jeweiligen Sicherheitsbedarf erfolgt. [2]Alternativ ist die Verwendung eines anderen, dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechenden Authentifizierungsverfahrens zulässig.

b) [1]Das Starten des IT-Systems darf nur mit dem dafür bereit gestellten Betriebssystem erfolgen. [2]Zu diesem Zweck sind geeignete technische Maßnahmen wie beispielsweise ein Boot-Schutz umzusetzen.

c) Sicherungskopien und Ausdrucke der Datenbestände sind vor Fremdzugriff und vor der gleichzeitigen Vernichtung mit den Originaldaten zu schützen.

d) [1]Die Daten der Schutzklasse II sind auf zentralen Systemen in besonders gegen unbefugten Zutritt gesicherten Räumen zu speichern, sofern keine begründeten Ausnahmefälle gegeben sind. [2]Diese sind schriftlich dem oder der betrieblichen Datenschutzbeauftragten zu melden. [3]Die jeweils beteiligten IT-Systeme sind dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen zu schützen. [4]Eine Speicherung auf anderen IT-Systemen darf nur erfolgen, wenn diese mit einem geeigneten Zugriffsschutz ausgestattet sind.

e) [1]Die Übermittlung personenbezogener Daten außerhalb eines geschlossenen und gesicherten Netzwerks (auch über automatisierte Schnittstellen) hat grundsätzlich verschlüsselt zu erfolgen. [2]Das Verschlüsselungsverfahren ist dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen auszuwählen.

§ 13
Datenschutzklasse III und Schutzniveau III

(1) [1]Der Datenschutzklasse III unterfallen personenbezogene Daten, deren missbräuchliche Verarbeitung die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann. [2]Hierzu gehören insbesondere die besonderen Kategorien personenbezogener Daten gemäß § 4 Ziffer 2. KDG sowie Daten über strafbare Handlungen, arbeitsrechtliche Rechtsverhältnisse, Disziplinarentscheidungen und Namens- und Adressangaben mit Sperrvermerken.

(2) [1]Zum Schutz der in die Datenschutzklasse III einzuordnenden Daten ist ein Schutzniveau III zu definieren. [2]Dieses setzt voraus, dass neben dem Schutzniveau II mindestens folgende Voraussetzungen gegeben sind:

a) [1]Ist es aus dienstlichen Gründen zwingend erforderlich, dass Daten der Datenschutzklasse III auf mobilen Geräten im Sinne des § 4 Absatz 2 oder Datenträgern gespeichert werden, sind diese Daten nur verschlüsselt abzuspeichern. [2]Das Verschlüsselungsverfahren ist dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen auszuwählen.

b) [1]Eine langfristige Lesbarkeit der zu speichernden Daten ist sicher zu stellen. [2]So müssen z.B. bei verschlüsselten Daten die Sicherheit des Schlüssels und die erforderliche Entschlüsselung auch in dem nach § 16 Absatz 1 zu erstellenden Datensicherungskonzept berücksichtigt werden.

§ 14
Umgang mit personenbezogenen Daten, die dem Beichtgeheimnis oder dem Seelsorgegeheimnis unterliegen

(1) [1]Personenbezogene Daten, die dem Beichtgeheimnis oder dem Seelsorgegeheimnis unterliegen, sind in besonders hohem Maße schutzbedürftig. [2]Ihre Ausspähung oder Verlautbarung würde dem Vertrauen in die Verschwiegenheit katholischer Dienststellen und Einrichtungen schweren Schaden zufügen.

(2) Das Beichtgeheimnis nach cc. 983 ff. CIC ist zu wahren; personenbezogene Daten, die dem Beichtgeheimnis unterliegen, dürfen nicht verarbeitet werden.

(3) Personenbezogene Daten, die, ohne Gegenstand eines Beichtgeheimnisses nach cc. 983 ff. CIC zu sein, dem Seelsorgegeheimnis unterliegen, dürfen nur verarbeitet werden, wenn dem besonderen Schutzniveau angepasste, erforderlichenfalls über das Schutzniveau der Datenschutzklasse III hinausgehende technische und organisatorische Maßnahmen ergriffen werden.

(4) [1]Eine Maßnahme im Sinne des Absatz 3 kann, wenn die Verarbeitung auf IT-Systemen erfolgt, insbesondere die Unterhaltung eines eigenen Servers bzw. einer eigenen Datenablage in einem Netzwerk ohne externe Datenverbindung sein. [2]Auch die verschlüsselte Abspeicherung der personenbezogenen Daten auf einem externen Datenträger, der außerhalb der Dienstzeiten in einem abgeschlossenen Tresor gelagert wird, kann eine geeignete technische und organisatorische Maßnahme darstellen.

(5) Erfolgt die Seelsorge außerhalb eines geschlossenen Netzwerkes, sind geeignete, erforderlichenfalls über das Schutzniveau der Datenschutzklasse III hinausgehende, technische und organisatorische Maßnahmen nach dem aktuellen Stand der Technik zu treffen.

(6) Die Absätze 3 bis 5 gelten auch für personenbezogene Daten, die in vergleichbarer Weise schutzbedürftig sind.

Kapitel 4
Maßnahmen des Verantwortlichen und des oder der Mitarbeitenden

§ 15
Maßnahmen des Verantwortlichen

(1) Verantwortlicher ist gemäß § 4 Nr. 9. KDG die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Ihm obliegt die Risikoanalyse zur Feststellung des Schutzbedarfs (§ 9 Absatz 1) sowie die zutreffende Einordnung der jeweiligen Daten in die Datenschutzklassen (§ 9 Absatz 6).

(3) Der Verantwortliche klärt die Mitarbeitenden über Gefahren und Risiken auf, die insbesondere aus der Nutzung eines IT-Systems erwachsen können.

(4) Der Verantwortliche stellt sicher, dass ein Konzept zur datenschutzrechtlichen Ausgestaltung der IT-Systeme erstellt und umgesetzt wird.

(5) [1]Erfolgt die Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter, so ist der Verantwortliche verpflichtet, die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters regelmäßig, mindestens jedoch im Abstand von jeweils zwei Jahren auf ihre Wirksamkeit zu überprüfen und dies zu dokumentieren. [2]Bei Vorlage eines anerkannten Zertifikats durch den Auftragsverarbeiter gemäß § 29 Absatz 6 KDG kann auf eine Prüfung verzichtet werden.

(6) [1]Der Verantwortliche kann, unbeschadet seiner Verantwortlichkeit, seine Aufgaben und Befugnisse nach dieser Durchführungsverordnung durch schriftliche Anordnung auf geeignete Mitarbeitende übertragen. [2]Eine Übertragung auf den betrieblichen Datenschutzbeauftragten oder die betriebliche Datenschutzbeauftragte ist ausgeschlossen.

§ 16
Maßnahmen des Verantwortlichen zur Datensicherung

(1) [1]Der Verantwortliche hat ein Datensicherungskonzept zu erstellen und entsprechend umzusetzen. [2]Dabei ist die langfristige Lesbarkeit der zu speichernden Daten in der Datensicherung anzustreben.

(2) [1]Zum Schutz personenbezogener Daten vor Verlust sind regelmäßige Datensicherungen erforderlich. [2]Dabei sind u.a. folgende Aspekte mit zu berücksichtigen:

a) Soweit eine dauerhafte Lesbarkeit der Daten im Sinne des § 4 Absatz 3 nicht auf andere Weise sichergestellt werden kann, sind Sicherungskopien der verwendeten Programme in allen verwendeten Versionen anzulegen und von den Originaldatenträgern der Programme und den übrigen Datenträgern getrennt aufzubewahren.
b) Die Datensicherung soll in Umfang und Zeitabstand anhand der entstehenden Auswirkungen eines Verlustes der Daten festgelegt werden.

(3) Unabhängig von der Einteilung in Datenschutzklassen sind geeignete technische Abwehrmaßnahmen gegen Angriffe und den Befall von Schadsoftware z.B. durch den Einsatz aktueller Sicherheitstechnik wie Virenscanner, Firewall-Technologien und eines regelmäßigen Patch-Managements (geplante Systemaktualisierungen) vorzunehmen.

§ 17
Maßnahmen des oder der Mitarbeitenden

[1]Unbeschadet der Aufgaben des Verantwortlichen im Sinne des § 4 Ziffer 9. KDG trägt jeder und jede Mitarbeitende die Verantwortung für die datenschutzkonforme Ausübung seiner Tätigkeit. [2]Es ist ihm oder ihr untersagt, personenbezogene Daten zu einem anderen als dem in der jeweils rechtmäßigen Aufgabenerfüllung liegenden Zweck zu verarbeiten.

Kapitel 5
Besondere Gefahrenlagen

§ 18
Nutzung von Cloud-Diensten

Für die Verarbeitung personenbezogener Daten mit einem Cloud-Dienst gilt ergänzend zu den Vorschriften der §§ 5 ff.:

(1) Es sind primär bereits geprüfte und freigegebene Cloud-Dienste zu nutzen.

(2) [1]Vor der Nutzung anderer Cloud-Dienste ist anhand nachfolgender Aspekte zu prüfen, ob die erforderlichen Sicherheitsanforderungen erfüllt werden. [2]Folgende Aspekte können ein erhöhtes Risiko darstellen:

a) ungeplante vorzeitige Vertragsbeendigung durch den Diensteanbieter,
b) unzureichend gesicherte administrative Zugänge,
c) mangelnde Portabilität von personenbezogenen Daten und IT-Systemen,
d) generelle Abhängigkeit vom Cloud-Diensteanbieter mangels Wechselmöglichkeit,
e) Gefährdung der Integrität von Informationen aufgrund herstellerspezifischer Datenformate,
f) gemeinsame Nutzung der Cloud-Infrastruktur durch mehrere Kunden,
g) Unkenntnis über den Speicherort der Informationen,
h) hohe Mobilität der Informationen sowie
i) unbefugter Zugriff auf Informationen beispielsweise durch Administrationspersonal des Cloud-Diensteanbieters oder Dritte.

(3) Vor der Nutzung des Cloud-Dienstes ist in Abhängigkeit von der Risikoanalyse eine Exit-Strategie zu definieren (z. B. Datenlöschung, Datenübertragung).

§ 19
Autorisierte Programme

Auf dienstlichen IT-Systemen dürfen ausschließlich vom Verantwortlichen autorisierte Programme und Kommunikationstechnologien verwendet werden.

§ 20
Nutzung dienstlicher IT-Systeme zu auch privaten Zwecken

[1]Die Nutzung dienstlicher IT-Systeme zu auch privaten Zwecken ist grundsätzlich unzulässig. [2]Ausnahmen regelt der Verantwortliche unter Beachtung der jeweils geltenden gesetzlichen Regelungen.

§ 21
Nutzung privater IT-Systeme zu dienstlichen Zwecken

(1) [1]Die Verarbeitung personenbezogener Daten auf privaten IT-Systemen zu dienstlichen Zwecken ist grundsätzlich unzulässig. [2]Sie kann als Ausnahme von dem Verantwortlichen unter Beachtung der jeweils geltenden gesetzlichen Regelungen zugelassen werden.

(2) [1]Die Zulassung erfolgt schriftlich und beinhaltet mindestens

a) die Angabe der Gründe, aus denen die Nutzung des privaten IT-Systems erforderlich ist,
b) eine Regelung über den Einsatz einer zentralisierten Verwaltung von Mobilgeräten (z.B. Mobile Device Management) auf dem privaten IT-System des oder der Mitarbeitenden,
c) das Recht des Verantwortlichen zur Löschung durch Fernzugriff aus wichtigem und unabweisbarem Grund; ein wichtiger und unabweisbarer Grund liegt insbesondere vor, wenn der Schutz personenbezogener Daten Dritter nicht auf andere Weise sichergestellt werden kann,
d) eine jederzeitige Überprüfungsmöglichkeit des Verantwortlichen,
e) die Dauer der Nutzung des privaten IT-Systems für dienstliche Zwecke,
f) das Recht des Verantwortlichen festzulegen, welche Programme verwendet oder nicht verwendet werden dürfen sowie
g) die Verpflichtung zum Nachweis einer Löschung der zu dienstlichen Zwecken verarbeiteten personenbezogenen Daten, wenn die Freigabe der Nutzung des privaten IT-Systems endet, das IT-System weitergegeben oder verschrottet wird.

[2]Ergänzend ist dem oder der betreffenden Mitarbeitenden eine spezifische Handlungsanweisung auszuhändigen, die Regelungen zur Nutzung des privaten IT-Systems enthält.

(3) Der Zugang von privaten IT-Systemen über sogenannte webbasierte Lösungen kann mit den Mitarbeitenden vereinbart werden, soweit alle datenschutzrechtlichen Voraussetzungen für eine sichere Nutzung gegeben sind.

(4) [1]Die Weiterleitung dienstlicher personenbezogener Daten auf private E-Mail-Konten ist unzulässig. [2]Dies gilt auch für personalisierte E-Mail-Adressen. [3]Ausnahmeregelungen können von dem Verantwortlichen getroffen werden, soweit das datenschutzrechtliche Schutzniveau, insbesondere nach dem KDG oder dieser Durchführungsverordnung, nicht unterschritten wird.

(5) Der oder die Mitarbeitende hat sicherzustellen, dass unberechtigte Dritte, insbesondere Familienmitglieder, keinen Zugriff auf dienstliche personenbezogene Daten haben.

§ 22
Externe Zugriffe, Auftragsverarbeitung

(1) [1]Der Zugriff aus und von anderen IT-Systemen durch Externe (z.B. externe Dienstleister, externe Dienststellen) schafft besondere Gefahren hinsichtlich der Ausspähung von Daten. [2]Derartige Zugriffe dürfen nur aufgrund vertraglicher Vereinbarung erfolgen. [3]Insbesondere mit Auftragsverarbeitern, die nicht den Regelungen des KDG unterfallen, ist grundsätzlich neben der Anwendung der EU-Datenschutzgrundverordnung die Anwendung des KDG zu vereinbaren.

(2) Bei Zugriffen durch Externe ist mit besonderer Sorgfalt darauf zu achten und nicht nur vertraglich, sondern nach Möglichkeit auch technisch sicherzustellen, dass keine Kopien der personenbezogenen Datenbestände gefertigt werden können.

(3) [1]Muss dem Externen bei Vornahme der Arbeiten ein Systemzugang eröffnet werden, ist dieser Zugang entweder zu befristen oder unverzüglich nach Beendigung der Arbeiten zu deaktivieren. [2]Im Zuge dieser Arbeiten vergebene Passwörter sind nach Beendigung der Arbeiten unverzüglich zu ändern.

(4) Bei der dauerhaften Inanspruchnahme von externen IT-Dienstleistern sind geeignete vergleichbare Regelungen zu treffen.

(5) [1]Eine Fernwartung von IT-Systemen darf darüber hinaus nur erfolgen, wenn der Beginn aktiv seitens des Auftraggebers eingeleitet wurde, über sichere Verbindungen erfolgt und die Fernwartung systemseitig protokolliert wird. [2]Im Falle der Einbeziehung externer Dienstleister sind auch die datenschutzrechtlichen Anforderungen und Verantwortlichkeiten sowie technische Schutzmaßnahmen vertraglich zu regeln.

(6) Die Verbringung von IT-Systemen mit Daten der Datenschutzklasse III zur Durchführung von Wartungsarbeiten in den Räumen eines Externen darf nur erfolgen, wenn die Durchführung der Wartungsarbeiten in eigenen Räumen nicht möglich ist und sie unter den Bedingungen einer Auftragsverarbeitung erfolgt.

§ 23
Verschrottung und Vernichtung von IT-Systemen, Abgabe von IT-Systemen zur weiteren Nutzung

(1) [1]Bei der Verschrottung bzw. der Vernichtung von IT-Systemen im Sinne des § 4 Abs. 2 Nr. 1 dieser Verordnung, insbesondere Datenträgern, Faxgeräten und Druckern, sind den jeweiligen DIN-Normen entsprechende Maßnahmen zu ergreifen, die die Lesbarkeit oder Wiederherstellbarkeit der Daten zuverlässig ausschließen. [2]Dies gilt auch für den Fall der Abgabe von IT-Systemen, insbesondere Datenträgern, zur weiteren Nutzung.

(2) Absatz 1 gilt auch für die Verschrottung, Vernichtung oder Abgabe von privaten IT-Systemen, die gemäß § 20 zu dienstlichen Zwecken genutzt werden.

§ 24
Passwortlisten der Systemverwaltung

Alle nicht zurücksetzbaren Passwörter (z.B. BIOS- und Administrationspasswörter) sind besonders gesichert aufzubewahren.

§ 25
Übermittlung personenbezogener Daten per Fax

[1]Die Übermittlung personenbezogener Daten per Fax ist grundsätzlich unzulässig. [2]In spezifischen Bestimmungen können Ausnahmen, insbesondere Übergangsbestimmungen, vorgesehen werden; dabei sind die Vorschriften der §§ 5 ff. und die jeweils aktuellen Sicherheitsstandards zu beachten.

§ 26
Sonstige Formen der Übermittlung personenbezogener Daten

(1) [1]E-Mails, die personenbezogene Daten der Datenschutzklasse II oder III enthalten, dürfen ausschließlich im Rahmen eines geschlossenen und gesicherten Netzwerks oder in verschlüsselter Form mit geeignetem Verschlüsselungsverfahren übermittelt werden. [2]Das Verschlüsselungsverfahren ist dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen auszuwählen.

(2) Eine Übermittlung personenbezogener Daten per E-Mail an Postfächer, auf die mehr als eine Person Zugriff haben (sog. Funktionspostfächer), ist in Fällen personenbezogener Daten der Datenschutzklassen II und III grundsätzlich nur zulässig, wenn durch vorherige Abstimmung mit dem Empfänger sichergestellt ist, dass ausschließlich autorisierte Personen Zugriff auf dieses Postfach haben.

(3) Für die Übermittlung von Video- und Sprachdaten insbesondere im Zusammenhang mit Video- und Telefonkonferenzen gilt Absatz 1 unter Berücksichtigung des aktuellen Standes der Technik entsprechend.

§ 27
Kopier- / Scangeräte

Bei Kopier-/Scangeräten mit eigener Speichereinheit ist sicherzustellen, dass ein Zugriff auf personenbezogene Daten durch unberechtigte Mitarbeitende oder sonstige Dritte nicht möglich ist.

Kapitel 6
Übergangs- und Schlussbestimmungen

§ 28
Inkrafttreten

Diese Durchführungsverordnung tritt zum 01.03.2019 in Kraft.

Erfurt, den 20.02.2019

gez. Raimund Beck
Generalvikar