KDG-Praxishilfe 15

Technischer Datenschutz

nach dem neuen Gesetz über den Kirchlichen Datenschutz (KDG)

Stand 11/2017

Konferenz der Diözesandatenschutzbeauftragten
der Katholischen Kirche Deutschlands

Inhalt

Praxishilfe 15

Technischer Datenschutz nach dem Kirchlichen Datenschutzgesetz (KDG)

Herausgegeben von
der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands

So erreichen Sie uns:

Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund
Tel. 0231 / 13 89 85 – 0
Fax 0231 / 13 89 85 – 22
E-Mail: info@kdsz.de
www.katholisches-datenschutzzentrum.de

Autor dieser Praxishilfe:
Der Diözesandatenschutzbeauftragte für die nordrhein-westfälischen (Erz-)Bistümer

Diese Praxishilfe der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands dient als erste Orientierung, wie nach Auffassung der Diözesandatenschutzbeauftragten das neue Gesetz über den kirchlichen Datenschutz (KDG) im praktischen Vollzug angewendet werden sollte. Sie kann noch keine verbindliche Auslegung bieten, sondern stellt die gegenwärtige Interpretation der neuen Vorschriften durch die Diözesandatenschutzbeauftragten dar.

Revision 1.0/ 22.12.2017

Technischer Datenschutz nach dem Kirchlichen Datenschutzgesetz (KDG)

1. Durchführung anhand der Regelungen aus KDO-DVO und KDG

Die bisher gültige Anordnung über den kirchlichen Datenschutz (KDO) wurde zum Thema „technisch-organisatorische Maßnahmen“ durch die zur KDO gehörenden Durchführungsverordnung (KDO-DVO) weiter konkretisiert und ausgeführt. Nach Wirksamwerden des KDG im Mai 2018 wird die KDO-DVO überarbeitet werden. Bis dahin behält die KDO-DVO weiterhin ihre Gültigkeit, längstens bis zum 30.06.2019. Die Durchführungsverordnung fordert acht technisch-organisatorische Maßnahmen:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungsgebot

In § 26 des neuen KDG werden die technisch-organisatorischen Maßnahmen wie folgt beschrieben bzw. werden aufgeführt:

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

Beide Listen lassen sich aber kombinieren, so dass die Anforderungen weiterhin abgeleitet werden können:

- Pseudonymisierung und Verschlüsselung
- Zugangskontrolle
- Zugriffskontrolle

- Weitergabekontrolle
- Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Verfügbarkeitskontrolle
- Wiederherstellung
- Überprüfung, Bewertung und Evaluierung
- PDCA Zyklus
- Auftragskontrolle
- Trennungsgebot

2. Pseudonymisierung und Verschlüsselung

Durch die **Pseudonymisierung** kann ein nachfolgender Verarbeiter von personenbezogenen Daten keine Rückschlüsse mehr auf die ursprüngliche Person ziehen.
Durch eine **Verschlüsselung** von Daten ist der Transport und die Aufbewahrung von Daten vor dem Zugriff durch unberechtigten Dritten geschützt. Diese erhalten nutzlose Zeichenfolgen. Voraussetzung ist ein aktuell sicherer Algorithmus und deren korrekten Implementierung.

3. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit

Die Vertraulichkeit von personenbezogener Daten kann sowohl durch organisatorische als auch technische Maßnahmen erreicht werden. So schränken entsprechende Zugriffsregeln den Zugriff auf den erforderlichen Personenkreis ein. Mit Hilfe von Verschlüsselung kann der Zugriff ohne das entsprechende Kennwort unterbunden werden.
Mit dem Einsatz von Hash Algorithmen kann die Integrität, also die Unverfälschbarkeit, nachgewiesen werden.

Der Datenverlust durch unbeabsichtigte Löschung und technisches Versagen muss durch entsprechende organisatorische und technische Maßnahmen verhindert werden. Hierzu zählt unter anderem das Erstellen von Backups.

Die Belastbarkeit ist im neuen KDG als weiteres Sicherheitsziel hinzugekommen. Die verantwortliche Stelle muss durch geeignete Maßnahmen, wie zum Beispiel ein Backup-Rechenzentrum oder Failover Clustering, einen technischen Ausfall kompensieren können.

4. Wiederherstellung

In Folge eines technischen Defekts oder einer Cyberattacke muss die verantwortliche Stelle in der Lage sein, die Daten ohne Verlust rasch wiederherzustellen.

5. Überprüfung, Bewertung und Evaluierung

Alle technischen und organisatorischen Maßnahmen müssen einer ständigen Evaluierung unterzogen werden. Dies ist unter anderem durch einen geänderten Betriebsablauf als auch durch neuartige Cyberattacken nötig. Ein mögliches Verfahren hierzu ist der PDCA Zyklus (siehe auch Praxishilfe 12).

6. Kontrollvorgaben

6.1 Zutrittskontrolle

Mit der Zutrittskontrolle soll der physische Zugang zu IT-Komponenten wie zum Beispiel Server, Switches und Telefonanlagen kontrolliert werden. Ein entsprechendes Schlüsselmanagement, sowohl analog als auch digital, ist vorzuhalten. Zutritte in gesicherte Räume, in welchen sich wichtige IT Infrastrukturkomponenten in Betrieb befinden, sollten protokolliert werden.

6.2 Zugangskontrolle

Jeder Benutzer muss eine eigene eindeutige Benutzerkennung im System erhalten. Dieser sollte mit einem entsprechenden komplexen Kennwort gesichert sein. Das Kennwort ist nach aktuellem Stand der Technik zu verschlüsseln. Nicht minder wichtig ist der Prozess, wie zum Beispiel der Benutzer bei Passwortverlust ein Ersatzkennwort erhält.
Zur Zugangskontrolle gehört ebenfalls das Patchmanagement aller eingesetzter Software und eine entsprechende Anti-Viren-Software.

6.3 Zugriffskontrolle

Durch ein entsprechendes Rechtemanagement kann der Zugriffsbereich auf personenbezogene Daten auf ein Minimum von Teilnehmern reduziert werden. Hier empfiehlt sich die Berechtigung nicht an Personen, sondern an die entsprechende Rolle zu knüpfen. Ein weiterer Baustein der Zugriffskontrolle ist zum Beispiel die Verschlüsselung der Festplatte von Computern. Somit kann ein Zugriff einer unberechtigten Person unterbunden werden.
Für den Fall der Fälle sollten entsprechende Vertretungsregeln im Vorfeld getroffen werden.

6.4 Weitergabekontrolle

Die Weitergabekontrolle erstreckt sich über ein weites technisches Themengebiet. Zum einen muss der Versand von Daten über das Internet geschützt werden. Zum anderen muss die Eindeutigkeit als auch die Vertraulichkeit gewahrt werden. Dies ist zum Beispiel mit entsprechender Technik wie zum Beispiel VPN, TLS und S/MIME möglich.
Auch stellt sich die Frage, wie die Transfers, als solches protokolliert werden. Dies kann zum Beispiel mit dem Logfile der Firewall oder in der Fachanwendung erfolgen. Das Reglementieren von Schnittstellen wie zum Beispiel USB oder das Einführen einer Data-Loss-Prevention-Software kann die unerlaubte Weitergabe von personenbezogenen Daten erschweren. Die Technik der Datei- und Festplattenverschlüsselung wurde bereits unter Zugriffskontrolle erwähnt.

6.5 Eingabekontrolle

Grundlage für die Eingabekontrolle ist die Identifizierung des Benutzers unter anderem mittels Benutzername und Kennwort. Wird ein Benutzername von mehreren Anwendern genutzt, ist eine korrekte Zuordnung von Eingaben zu einem Benutzer nicht mehr möglich und aus diesem Grunde zu unterlassen. Die Protokolle zur Eingabekontrolle müssen jedoch auf ein Minimum reduziert und mit den entsprechenden Zugriffsberechtigungen versehen werden, damit keine Mitarbeiterüberwachung erfolgen kann.

6.6 Auftragskontrolle

Für die Verarbeitung von Daten über einen Auftragsnehmer muss ein entsprechender Vertrag zur Auftragsverarbeitung geschlossen werden. Dieser beinhaltet den gesamten Lebenszyklus der Dateninklusive der Löschung. So müssen in dem Vertrag weisungsbefugte Personen und die Meldeform genannt werden. Der betriebliche Datenschutzbeauftragte muss sich über geeignete Maßnahme von der Einhaltung der Datenschutzanforderung überzeugen. Zu berücksichtigen sind auch die Unterauftragsverhältnisse, diese sollten im Vertrag zur Auftragsverarbeitung mit aufgenommen werden.
Die beschriebenen Inhalte müssen nicht nur bei aktiver Verarbeitung, sondern auch bei einer Fernwartung mit möglicher Einsichtnahme durch den die Fernwartung Durchführenden beachtet werden.

6.7 Verfügbarkeitskontrolle

Die verantwortliche Stelle, beziehungsweise deren IT-Abteilung, muss für eine hohe Verfügbarkeit sorgen. Dieses umfasst zum einen das Erstellen von Backups, inklusive des Tests der Wiederherstellung, als auch die Möglichkeit einer Ausweichmöglichkeit. Dieses muss im Zuge der Risikobeurteilung festgelegt werden.

7. Trennungsgebot

Werden Anwendungen von verschiedenen Einrichtungen auf der gleichen technischen Plattform betrieben, so muss das Trennungsgebot eingehalten werden. Die Nutzergruppen dürfen nur Daten der eigenen Einrichtung erreichen und einsehen können. Diese Trennung kann auf den IT Systemen physikalisch als auch logisch erfolgen. In Zeiten von Cloud Computing ist eine laufende Prüfung auf Einhaltung des Trennungsgebotes unausweichlich und strikt einzuhalten. Hier können ständige Soll-Ist Abgleiche oder Penetrationstests helfen.

Die in diesem Dokument beschriebenen Aufgaben und Maßnahmen sind nicht nur in Gesetzen wie dem KDG oder der europäischen Datenschutz Grundverordnung (DS-GVO) zu finden. Sie sind auch Bestandteil diverser Zertifizierungsnormen, wie z. B. der ISO 270XX oder in den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen IT-Grundschutzkatalogen aufgeführt.

8. Gesetzestext von §§ 26 und 27 KDG (VDD Beschlussfassung vom 20.11.2017)

§ 26
Technische und organisatorische Maßnahmen

(1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung unter anderem des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und einen Nachweis hierüber führen zu können. Diese Maßnahmen schließen unter anderem ein:

a) die Pseudonymisierung, die Anonymisierung und die Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicher-zustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(3) Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

(4) Die Einhaltung eines nach dem EU-Recht zertifizierten Verfahrens kann als Faktor her-angezogen werden, um die Erfüllung der Pflichten des Verantwortlichen gemäß Absatz 1 nachzuweisen.

(5) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte um sicherzustellen, dass ihnen unterstellte Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach kirchlichem oder staatlichem Recht zur Verarbeitung verpflichtet.

§ 27
Technikgestaltung und Voreinstellungen

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung technische und organisatorische Maßnahmen, die geeignet sind, die Datenschutzgrundsätze wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieses Gesetzes zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft technische und organisatorische Maßnahmen, die geeignet sind, durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, zu verarbeiten. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maß-nahmen müssen insbesondere geeignet sein, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(3) Ein nach dem EU-Recht genehmigtes Zertifizierungsverfahren kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 genannten Anforderungen nachzuweisen.

Raum für Ihre Notizen

Weitere Praxishilfen:

01 Wichtige Schritte bis zum In-Kraft-Treten des KDG

02 Der betriebliche Datenschutzbeauftragte nach dem KDG

03 Verantwortlichkeiten nach dem KDG

04 Auftragsverarbeitung nach dem KDG

05 Verzeichnis der Verarbeitungstätigkeiten nach dem KDG

06 Betroffenenrechte nach dem KDG

07 Transparenz- und Dokumentationspflichten nach dem KDG

08 Datenübermittlung in Drittländer

09 Befugnisse und Sanktionsmöglichkeiten der Aufsicht nach dem KDG

10 Umgang mit Datenpannen nach dem KDG

11 Datenschutzfolgeabschätzung nach dem KDG

12 Neue Anforderungen an die IT-Sicherheit nach dem KDG

13 Datenschutzorganisation und -managementsysteme nach dem KDG

14 Der Rechtsweg nach der KDSGO

16 Begriffe im neuen KDG

17 Rechtmäßigkeit der Verarbeitung/Einwilligung

18 Nutzung der Daten für Werbezwecke

Diese Schriftenreihe wird gemeinsam herausgegeben von

Diözesandatenschutz-
beauftragter für die nord-
deutschen (Erz-)Diözesen

Diözesandatenschutz-
beauftragter für die ost-
deutschen (Erz-)Diözesen

Diözesandatenschutzbeauftragter für die
nordrhein-westfälischen (Erz-)Diözesen

Diözesandatenschutzbeauftragter
für die bayerischen (Erz-)Diözesen

Gemeinsame Datenschutzstelle der (Erz-)Diözesen
Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stutt-
gart, Speyer und Trier