KDG-Praxishilfe 12

Neue Anforderungen an die IT-Sicherheit

nach dem neuen Gesetz über den Kirchlichen Datenschutz (KDG)

Stand 11/2017

Konferenz der Diözesan-datenschutzbeauftragten
der Katholischen Kirche Deutschlands

Inhalt

Praxishilfe 12

Neue Anforderungen an die IT-Sicherheit 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

Neue Anforderungen an die IT-Sicherheit nach dem Kirchlichen Datenschutzgesetz (KDG)

Technische und organisatorische Schutzmaßnahmen bei der Verarbeitung von personenbezogenen Daten sind essentiell für die Sicherheit und den Schutz der Daten. Die Anforderungen an den Schutz sind in verschiedenen Stellen im Gesetz genannt, z.B. bei der Auftragsverarbeitung in § 26 KDG.

1. Schutzbedarf und Risikoanalyse der personenbezogenen Daten

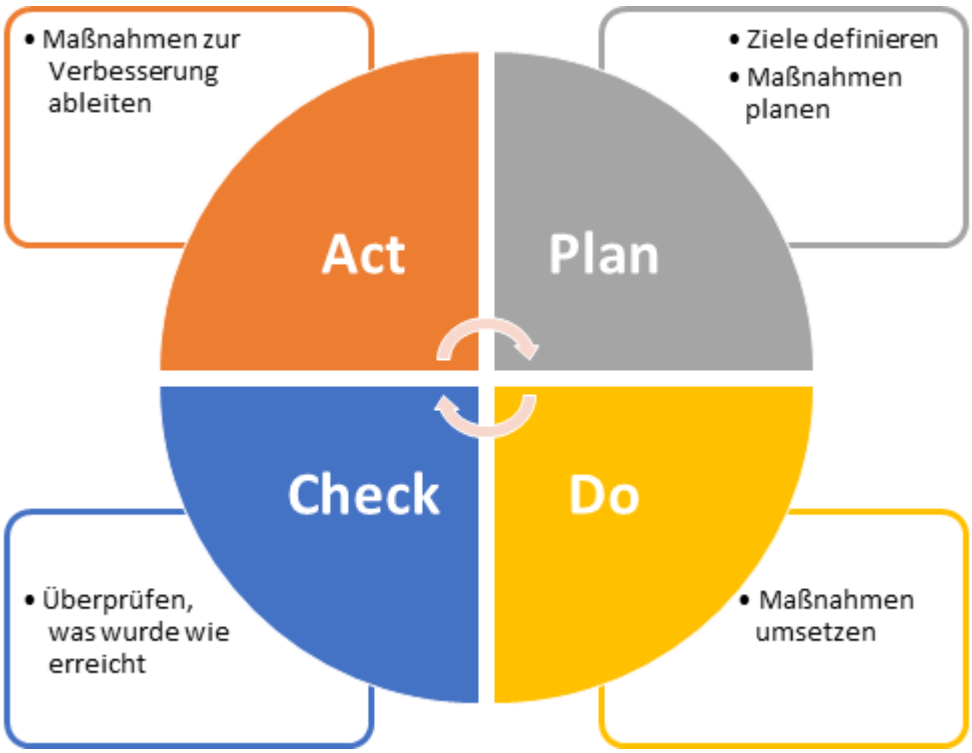
In § 26 Abs. 2 KDG z.B. fordert der Gesetzgeber eine Analyse der Risiken, die mit der Verarbeitung der personenbezogenen Daten verbunden sind. Objektive Kriterien für die Eintrittswahrscheinlichkeit und Schwere eines Schadens für die Rechte und Freiheiten natürlicher Personen (Betroffener) müssen hierbei herangezogen werden. Die Betrachtung gilt sowohl für die verantwortliche Stelle als auch für den Auftragsverarbeiter. Das Ergebnis dieser Analyse spiegelt sich in den entsprechenden technischen und organisatorischen Maßnahmen wieder. In der Praxis haben sich hierfür klar definierte Schutzklassen etabliert, welche ein normales, hohes oder sehr hohes Schutzniveau festlegen. Dabei kann die Anzahl und Benennung der Schutzklassen in jeder Einrichtung unterschiedlich sein. Die technischen Schutzmerkmale müssen nicht nur zum Zeitpunkt der Einführung und Erhebung dem Stand der Technik entsprechen, sondern auch während der gesamten Verarbeitungszeit bis hin zur Löschung. Techniken wie zum Beispiel Anonymisierung oder die Verschlüsselung können hierzu genutzt werden. Mit Pseudonymisierung können Sie den Benutzerkreis mit Zugriff auf die Klarnamen der personenbezogenen Daten verkleinern. Der Einsatz der entsprechenden Verfahren muss in der Verhältnismäßigkeit stimmig sein. Wird die Verarbeitung personenbezogener Daten an einen Auftragsverarbeiter übergeben, so hat die verantwortliche Stelle die Pflicht, die technisch-organisatorischen Maßnahmen des Auftragnehmers zu prüfen. Dies kann auch durch das Vorlegen eines anerkannten Zertifikats erfolgen. Die Auftragsverarbeitung wird ausführlich in der Praxishilfe 4 behandelt.

Sollen sensible personenbezogene Daten in einem neuen IT-System verarbeitet werden, so muss eine Datenschutz-Folgenabschätzung erfolgen. Auch zu diesem Thema wurde eine Praxishilfe (Nr. 11 Datenschutzfolgeabschätzung nach dem KDG) verfasst.

2. Schutzziele im Sicherheitsumfeld

Neben den Schutzzielen der Vertraulichkeit, Integrität und Verfügbarkeit, welche bereits in der KDO gefordert waren, gibt der Gesetzgeber nun auch vor, die Belastbarkeit der Systeme und Dienste sicherzustellen. Das bedeutet, dass die verantwortliche Stelle in Zusammenarbeit mit der IT-Abteilung ausreichende Ressourcen sowohl für die zutreffende Grundlast, als auch für eine bzw. die erwartbare Spitzenlast zur Verfügung stellen muss. Die Einführung eines „Business Continuity Management Systems“ unterstützt die Erfüllung dieser Forderung an die Belastbarkeit. Sollte es doch zu einem Zwischenfall kommen, der den Zugang zu den personenbezogenen Daten verhindert, ist eine schnelle entsprechende Wiederherstellung zu gewährleisten. Dieses ist unter anderem mit entsprechenden Backups und Notfallplänen zu erreichen.

Aus § 27 Abs. 1 KDG leitet sich ab, dass die gesamten technischen und organisatorischen Maßnahmen in einem ständigen PDCA (Plan Do Check Act) Zyklus zu prüfen sind.



3. Risikoanalyse

Um das entsprechende Schutzniveau der personenbezogenen Daten festzulegen, ist eine entsprechende Gefährdungsanalyse zu erstellen. Techniken wie zum Beispiel Backups, revisionssicheres Speichern und der sichere Datentransport sind für das Erreichen des nötigen Schutzniveaus notwendig. Die eingesetzte Technik muss im Verhältnis zum Schutzziel gewählt werden. Entsprechende aussagekräftige Zertifizierungen können die umgesetzten Maßnahmen dokumentieren.

4. Privacy by design, Privacy by default

Bei Inbetriebnahme von neuen IT-Systemen und Anwendungen oder deren Entwicklung ist darauf zu achten, dass die Erhebung von personenbezogenen Daten als Standardeinstellung auf ein Minimum zu reduzieren ist (privacy by default, privacy by design). So sollte der Benutzer aktiv seine Einwilligung für die Erfassung von personenbezogenen Daten geben, in dem zum Beispiel eine Checkbox auf einer Internetseite nicht bereits mit einem Haken aktiviert ist. Der Erwägungsgrund 78 der DS-GVO schreibt hierzu folgendes:

> *„Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden.“*

5. Löschkonzept

Daten, die zur Verarbeitung nicht mehr benötigt werden, müssen gelöscht werden. Ist der Aufwand zur Löschung unverhältnismäßig hoch, so ist der Zugriff auf diese Daten einzuschränken (Einschränkung der Verarbeitung [§4 Nr. 4 KDG] entspricht dem Sperren aus § 2 Abs. 4 Nr. 4 KDO). Um die Löschung sicher zu gewährleisten, empfiehlt sich hier ein entsprechendes Löschkonzept zu entwickeln. Durch ein Löschkonzept wird unter anderem der Speicherort von Daten klar dokumentiert. Dies erleichtert die Bearbeitung für den Fall, das ein Betroffener ein Auskunftsersuchen stellt, bei dem Sie alle seine Daten offenlegen müssen, inklusive der in allen Subsystemen gespeicherten Daten. In der Praxishilfe 6 zu den Betroffenenrechten finden Sie weitere Informationen.

6. Information Security Management System (ISMS)

Um die oben genannten Themen stringent in Ihrer Einrichtung umzusetzen, empfiehlt sich die Einführung eines Managements für Informationssicherheit (ISMS). Dies greift Hand in Hand mit dem Datenschutzmanagementsystem, über das eine weitere Praxishilfe informiert (Nummer 13 „Datenschutzorganisation und -managementsysteme nach dem KDG“). Mit diesem Instrument legen Sie klare Zuständigkeiten und Aufgaben fest. Mit der Einführung von Data Leak Prevention Systemen kann die bewusste oder unbewusste Weitergabe von personenbezogenen Daten unterbunden werden. Durch entsprechende Richtlinien, wie zum Beispiel Dienstanweisungen, kann die Einrichtungsleitung den Mitarbeitern ein Handwerkszeug an die Hand geben, damit diese sicher mit den IT-Betriebsmitteln umgehen kann. Dies kann zum Beispiel die Untersagung der Nutzung der dienstlichen E-Mail-Adresse für private Zwecke sein. Um dies weiterzuführen bedarf es einer ständigen Sicherheitsschulung aller Mitarbeiter und insbesondere der IT-Abteilung, damit diese aktuelle Angriffsvektoren kennt und unterbinden können.

7. Überprüfung der Maßnahmen

Mit einer IST-Überprüfung (Penetration-Test) können Sie Ihren aktuellen Stand in der IT-Sicherheit feststellen und bei Abweichungen gegebenenfalls durch geeignete Maßnahmen optimieren. In der Praxis hat sich gezeigt, dass u.a. die kontinuierliche Prüfung von Zugriffsrechten unerlässlich ist. Nicht selten kommt es vor, dass besonders Auszubildende bei einem fehlenden Prüfprozess zum Ende Ihrer Tätigkeit in der Einrichtung mehr Zugriffsberechtigungen auf Daten besitzen als andere Mitarbeiter.

Um zu prüfen, ob alle Maßnahmen im Notfall auch wirklich ineinandergreifen, sollte es realitätsnahe Übungen geben. Durch einen ständigen PDCA-Zyklus kommt es zu einer kontinuierlichen Verbesserung der IT-Sicherheit.

Das ISMS erfordert eine lückenlose Dokumentation der Prozesse und Abläufe, aus dem sich ein Notfallkonzept ergeben sollte. Die so gewonnenen Dokumentation dient ebenfalls der Rechenschaftspflicht aus dem KDG.

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

13 Datenschutzorganisation und -managementsysteme nach dem KDG

14 Der Rechtsweg nach der KDSGO

15 Technischer Datenschutz nach dem KDG

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