KDG-Praxishilfe 10

Umgang mit Datenpannen

nach dem neuen Gesetz über den Kirchlichen Datenschutz (KDG)

Stand 11/2017

Konferenz der Diözesan-datenschutzbeauftragten
der Katholischen Kirche Deutschlands

Inhalt

Praxishilfe 10

Umgang mit Datenpannen 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 0.1 / 08.12.2017

Umgang mit Datenpannen nach dem Kirchlichen Datenschutzgesetz (KDG)

Es ist schnell passiert ...

Der Verlust von personenbezogenen Daten oder die unberechtigte Kenntnisnahme dieser Daten durch Unbefugte können jede Einrichtung und jeden Verantwortlichen treffen. Wie schnell ist eine Datei an den falschen Mail-Adressaten geschickt, die Patientenausdrucke in den (einfachen) Papiermüll geworfen oder Daten in einer Papierakte oder am Bildschirm von Unbefugten eingesehen. Auch bei Angriffen auf die technische Infrastruktur der Einrichtung können personenbezogene Daten von Servern abgezogen werden.

Neue Meldepflicht eigentlich nicht neu

Im Bundesdatenschutzgesetz (BDSG) gibt es eine Meldepflicht für Datenpannen schon seit einigen Jahren im § 42a BDSG. Diese Vorschrift sah aber relativ hohe Hürden vor, bevor eine Meldepflicht der Datenpanne eintrat. Außerdem wurde diese Vorschrift nicht in die Anordnung über den kirchlichen Datenschutz (KDO) übernommen.

Meldepflicht jetzt auch im kirchlichen Bereich

Die neue Datenschutzgrundverordnung sieht in den Artikeln 33 und 34 (DS-GVO) jetzt eine Meldepflicht mit niedrigeren Voraussetzungen für die Meldung vor. Diese Regelung findet sich im neuen Gesetz über den kirchlichen Datenschutz (KDG) auch in den §§ 33 und 34 wieder.

> *§ 33 Abs. 1 KDG: Der Verantwortliche meldet der Datenschutzaufsicht unverzüglich die Verletzung des Schutzes personenbezogener Daten, wenn diese Verletzung eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt. […]*

Dabei sieht die Regelung in § 33 Abs. 1 KDG vor, dass die Meldung an die Datenschutzaufsicht immer zu erfolgen hat, wenn die Verletzung des Schutzes personenbezogener Daten eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt.
Hingegen hat eine Information der Betroffenen über die Verletzung des Schutzes personenbezogener Daten nach § 34 Abs. 1 KDG nur zu erfolgen, wenn ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge hat. Diese Abwägung kann für verschiedene Betroffene durchaus unterschiedliche Ergebnisse haben.

> *§ 34 Abs. 1 KDG: Hat die Verletzung des Schutzes personenbezogener Daten voraus-sichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.*

Die Information muss in einfacher und klarer Sprache abgefasst sein und bestimmte, in § 34 Abs. 2 KDG näher genannte Inhalte enthalten.

Der Verantwortliche hat die Verletzung der personenbezogenen Daten einschließlich der damit zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Maßnahmen zu dokumentieren (siehe § 33 Abs. 5 KDG). Diese Dokumentation muss der Datenschutzaufsicht die Überprüfung der Einhaltung der Vorgaben des § 33 KDG ermöglichen.

Ist jeder Vorfall meldepflichtig?

Das Gesetz geht davon aus, dass jede Verletzung gegenüber der Aufsicht meldepflichtig ist, die eine Gefahr für die Rechte und Freiheiten der betroffenen Personen darstellt. Das Gesetz unterscheidet dabei nicht zwischen Einzelfall und massenhaftem Datenverlust, nicht zwischen fahrlässiger oder vorsätzlicher Verletzung, nicht zwischen dem Verlust „normaler“ oder „besonderer“ personenbezogener Daten.

Damit diese Verpflichtung für die Einrichtungen auch erfüllbar bleibt, werden die Aufsichtsbehörden sich hier noch abstimmen und Hilfestellungen zur Risikobewertung und der Meldepflicht erarbeiten.

Gegenüber den Betroffenen kann die Informationspflicht gemäß § 34 Abs. 3 KDG entfallen, wenn der Verantwortliche geeignete Maßnahmen ergriffen hat oder ergreift, die eine Gefährdung der Rechte und Freiheiten der Betroffenen wirksam verhindern. Die Wirksamkeit dieser Maßnahmen wird im konkreten Fall zu bewerten sein.

Sofern die Einzelinformation der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, kann auch eine öffentliche

> *§ 34 Abs. 3 KDG:*
> *Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:*
> *a) Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen getroffen und auf die von der Verletzung betroffenen personenbezogenen Daten angewandt, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;*
> *b) der Verantwortliche hat durch nachträglich getroffene Maßnahmen sichergestellt, dass die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 nicht mehr gefährdet sind; [...]*

Bekanntmachung oder eine ähnliche, gleich wirksame Maßnahme gemäß § 34 Abs. 3 Buchst. c) KDG erforderlich sein.

Wie schnell muss die Meldung erfolgen?

Die Meldung an die Datenschutzaufsicht muss gemäß § 33 Abs. 1 KDG innerhalb von 72 Stunden erfolgen. Nur in begründeten Ausnahmefällen kann diese Frist überschritten

> *§ 33 Abs. 3 KDG: Die Meldung gemäß Absatz 1 enthält insbesondere folgende Informationen:*
> *a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;*
> *b) den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;*
> *c) eine Beschreibung der möglichen Folgen der Verletzung des Schutzes personenbezogener Daten;*
> *d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.*

werden. Die Meldung hat die aus § 33 Abs. 3 KDG ersichtlichen umfassenden Angaben zu enthalten. Sofern die Informationen nach § 33 Abs. 3 KDG nicht schon alle mit der Meldung bereitgestellt werden können, sind diese unverzüglich nachzureichen (§ 33 Abs. 4 KDG).

Gilt die Informationspflicht auch für Auftragsverarbeiter?

Der Auftragsverarbeiter, dem eine Verletzung des Schutzes personenbezogener Daten bekannt wird, hat dies gemäß § 33 Abs. 2 KDG unverzüglich dem Verantwortlichen zu melden.

Was soll schon passieren, wenn ich keine Meldung mache und die Betroffenen nicht informiere?

Kommt der Verantwortliche der eigentlich notwendigen Information an die Betroffenen nicht nach, so kann die Datenschutzaufsicht verlangen, dass die Information nachgeholt wird (vgl. § 34 Abs. 4 KDG). Ebenso kann die Datenschutzaufsicht feststellen, dass einer der Gründe des § 34 Abs. 3 KDG vorliegt und eine Meldung nicht notwendig ist (vgl. § 34 Abs. 4 KDG). Das Unterlassen einer gemäß § 33 KDG notwendigen Meldung an die Datenschutzaufsicht

oder einer gemäß § 34 KDG notwendigen Information der Betroffenen könnte mit einem Bußgeld nach § 51 KDG geahndet werden.

Außerdem könnte der Verantwortliche gemäß § 50 KDG für Schäden der Betroffenen haften oder Schadensersatzpflichtig werden, wenn durch die unterlassene Information ein Schaden beim Betroffenen entsteht oder vergrößert wird.

Weitere Informationen

Die Diözesandatenschutzbeauftragten werden bis zum Inkrafttreten des neuen KDG noch weitere Informationen zu Voraussetzungen und Umfang der Melde- und Informationspflicht herausgeben.

Bei Fragen können Sie sich gerne an Ihre zuständige Datenschutzaufsicht wenden.

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

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

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