Arbeitshilfe

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

Stand 03/2019

Katholisches Datenschutzzentrum

Inhalt

Arbeitshilfe

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

Herausgegeben vom Katholischen Datenschutzzentrum

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

Diese Arbeitshilfe des Katholischen Datenschutzzentrums der nordrhein-westfälischen (Erz-)Diözesen dient als erste Orientierungshilfe, wie die Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) im praktischen Vollzug angewendet werden sollte. Sie kann keine verbindliche Auslegung bieten, sondern stellt die gegenwärtige Interpretation der neuen Vorschriften durch das Katholische Datenschutzzentrum dar.

Revision 1.0 / 02.04.2019

Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz

1. Gesetzgebung

Der Verband der Diözesen Deutschlands (VDD) hat in seiner Vollversammlung am 19. November 2018 die Musterfassung der Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) beschlossen. Die KDG-DVO folgt der bisherigen Durchführungsverordnung zur vorherigen Anordnung über den kirchlichen Datenschutz, der KDO-DVO, nach und löst diese ab. Für die Inkraftsetzung der KDG-DVO war die Besonderheit im katholischen kirchlichen Recht, wonach der jeweilige Diözesanbischof Gesetzgeber seiner (Erz-)Diözese ist, zu berücksichtigen. Vergleichbar gilt dies für Verordnungen, die durch den jeweiligen Generalvikar einer (Erz-)Diözese in Kraft gesetzt werden können, da sich dessen Rechtssetzungsbefugnis von Gesetzgebungskompetenz des Diözesanbischofs ableitet. Die Befugnis zur Schaffung einer Rechtsgrundlage für den Regelungsbereich der aktuellen KDG-DVO hatten die Diözesanbischöfe in § 56 KDG der jeweiligen diözesanen Fassung geschaffen, wonach zur Durchführung des KDG erforderliche Regelungen durch den Generalvikar getroffen werden können. Dementsprechend erfolgt die Umsetzung des Musters in diözesanes Recht mit Wirkung zum 01. März 2019. Auf dieses einheitliche Datum für das Inkrafttreten hatten sich die Bischöfe in der Vollversammlung des Verbands der Diözesen Deutschlands (VDD) am 19. November 2018 verständigt.

2. Allgemeine Hinweise zu den Änderungen

In § 27 KDG-DVO sieht der Verordnungsgeber vor, dass die Regelungen unverzüglich umzusetzen sind, wobei durch die Festlegung eines Endtermins zum 31. Dezember 2019 eine Frist bis zu einer endgültigen Umsetzung eingeräumt wird. Insoweit besteht bis zum Ablauf dieser zeitlichen Vorgabe noch eine gewisse „Schonfrist" für die Umsetzung der Inhalte der Verordnung. Diese Frist sollte jedoch von den kirchlichen Stellen auch für die Realisierung genutzt werden, damit später nicht mit entsprechendem Zeitdruck umgesetzt werden muss und Versäumnisse oder Überschreitungen der Fristen drohen.

Mit der neuen Durchführungsverordnung hat der Verordnungsgeber im Gegensatz zur Vorgängerregelung eine klarer strukturierte Fassung verabschiedet. Die KDG-DVO beinhaltet Konkretisierungen der Vorgaben des Gesetzes über den Kirchlichen Datenschutz (KDG). Die Durchführungsverordnung beschreibt Anforderungen näher, so etwa im Fall der Risikoanalyse oder bezüglich der Erarbeitung von Datenschutzkonzepten und Datensicherungskonzepten und der Erstellung von Verzeichnissen von Verarbeitungstätigkeiten.

Die bereits durch das KDG vorgegebene Verantwortlichkeit der Verantwortlichen im Sinne des Gesetzes wird durch die KDG-DVO aufgegriffen und an verschiedenen Stellen hervorgehoben. Der Verantwortliche kann sich - im Rahmen der Wahrnehmung seiner Aufgaben und Letztverantwortung der Organisation - der Abteilungen und Stellen seiner Einrichtungen zu seiner Unterstützung bedienen, muss aber sicherstellen, dass die Entscheidungsabläufe bei ihm zusammentreffen und er die endgültige Entscheidung trifft, die auch seiner Gesamtverantwortung entspricht.

Beibehalten worden ist z. B. die Anforderung, die in einer Einrichtung verarbeiteten personenbezogenen Daten in Kategorien einzuteilen, konkret in die in der Verordnung näher beschriebenen Datenschutzklassen I - III, vergleiche §§ 9 ff KDG-DVO.

3. Verpflichtung auf das Datengeheimnis und Belehrung von Mitarbeitern

Die Anforderungen aus § 5 KDG, Mitarbeitende zu belehren und sie auf das Datengeheimnis zu verpflichten, werden in der Durchführungsverordnung konkretisiert. Ehrenamtlich tätige Personen sind neben den Beschäftigten von dem Begriff der Mitarbeiter mitumfasst, so dass auch diese in geeigneter Weise mit den Vorschriften des KDG und den weiteren Datenschutzbestimmungen vertraut zu machen sind. Dabei müssen die Mitarbeiter mit auf den konkreten Aufgabenbereich zugeschnittene Informationen versehen werden, so dass gegebenenfalls unterschiedliche und spezielle Belehrungen vorzunehmen sind. Von diesem Personenkreis ist in nachweisbarer Form eine Verpflichtungserklärung einzufordern, die zur Personalakte oder den entsprechenden Unterlagen des Mitarbeitenden genommen werden muss. Der konkrete Inhalt der Erklärung wird in § 3 der Durchführungsverordnung vorgegeben. Der Verordnungsgeber hat vorgesehen, dass die zuständigen Datenschutzaufsichten Muster für die Verpflichtungserklärung zur Verfügung stellen können. Diese bilden dann einen Mindeststandard, der nicht unterschritten werden darf. Zur Erleichterung für die Verantwortlichen und die kirchlichen Stellen ist in der Durchführungsverordnung festgelegt worden, dass bisherige

Verpflichtungserklärungen nach § 4 KDO auch weiterhin wirksam bleiben, so dass alleine wegen des neuen Gesetzes keine erneuten Verpflichtungserklärungen abgegeben werden müssen.

4. Mustervorgaben

Die Durchführungsverordnung enthält selbst keine Muster mehr, wie es etwa für die Verpflichtungserklärung in der Vorgängerverordnung der Fall war, da die Aufnahme von Mustern in die Verordnung bedeuten würde, dass bei notwendigen Formulierungsänderungen die KDG-DVO insgesamt dem erforderlichen Gesetzgebungsverfahren unterzogen werden müsste. Dies ist mit Blick auf eine denkbare Änderung einzelner Worte zu aufwendig. Daher ist vorgesehen, dass die zuständigen Datenschutzaufsichten Muster zur Verfügung stellen können. Sofern dies der Fall ist, bilden diese den Mindeststandard. Verantwortliche können entsprechend den gesetzlichen Vorgaben eigenständig Formulierungen entwickeln und verwenden. Jedoch ist dabei zu beachten, dass im Fall des Vorliegens von Mustern der Datenschutzaufsichten das darin vorgegebene Datenschutzniveau nicht unterschritten wird.

5. Begriffserläuterungen und Vorgaben

Die neue Durchführungsverordnung erläutert Begriffe wie „IT-Systeme“ und legt die Grundsätze der Verarbeitung in allgemeiner Form fest.

Darüber hinaus wird unter Bezugnahme auf die grundsätzlich zu beachtenden Vorgaben der §§ 26, 27 KDG näher ausgeführt, welche technischen und organisatorischen Maßnahmen von den Verantwortlichen zu treffen sind. Diese Vorgaben sind in der KDG-DVO näher dargestellt, wobei deutlich auf die Erfordernisse der notwendigen Kontrollen im Zusammenhang mit der Verarbeitung personenbezogener Daten und der Sicherstellung des technischen Datenschutzes hingewiesen wird.

In die Verordnung ist jetzt auch ausdrücklich aufgenommen worden, dass die getroffenen technischen und organisatorischen Maßnahmen durch den Verantwortlichen regelmäßig einer Überprüfung unterzogen werden müssen. Grundsätzlich ist es von der Notwendigkeit und den besonderen einzelnen Anforderungen vor Ort abhängig, in welchen Abständen diese regelmäßige Überprüfung erfolgen muss. Dabei ist der Verantwortliche gefordert, die Sensibilität der in seiner Einrichtung verarbeiteten personenbezogenen Daten zu berücksichtigen. Der Verordnungsgeber hat ihm darüber hinaus die Verpflichtung auferlegt, dass spätestens in einem Abstand von zwei Jahren die

Wirksamkeit der getroffenen Maßnahmen überprüft werden muss. Diese Überprüfung ist auch zu dokumentieren. Die Vorlage derartiger Dokumentationen wird sicherlich im Rahmen von Prüfungen durch die zuständige Datenschutzaufsicht verlangt werden.

6. Verzeichnis von Verarbeitungstätigkeiten

Der Verordnungsgeber greift hier die bereits im KDG enthaltenen Vorgaben auf. Die Verzeichnisse von Verarbeitungstätigkeiten sind durch die Verantwortlichen zu organisieren. Unter Beachtung der Übergangsfristen des § 57 Absatz 4 KDG betont die KDG-DVO noch einmal die erforderliche Anpassung der bisherigen Verfahrensverzeichnisse bzw. die Aufstellung neuer Verzeichnisse von Verarbeitungstätigkeiten bis spätestens 30. Juni 2019.

Der Verordnungsgeber legt in der Verordnung selbst keine genauen Vorgaben zur Umsetzung bei der Erstellung der Verzeichnisse fest. Er verweist aber auf die Möglichkeit, dass die Datenschutzaufsichten entsprechende Muster als Angebot zur Verfügung stellen. Sofern solche Muster existieren, bilden sie das Mindestniveau, welches im Rahmen der Verzeichniserstellung mindestens einzuhalten ist. Die derzeitigen Muster für die Verzeichnisse von Verarbeitungstätigkeiten des Katholischen Datenschutzzentrums sind zweigeteilt und sehen einerseits die zwingend aufzuführenden Elemente gemäß den Vorgaben des KDG und der KDG-DVO vor. Sie enthalten jedoch auch für die Informationsgewinnung des Verantwortlichen sinnvolle und nützliche Punkte, welche er gegebenenfalls zusätzlich in sein Verzeichnis aufnehmen sollte. Inhaltlich sind in jedem Fall die Vorgaben des § 31 KDG zu erfüllen.

Neu ist die Verpflichtung der Verantwortlichen, sich mit den Verzeichnissen von Verarbeitungstätigkeiten in regelmäßigen Abständen befassen zu müssen. Der Verantwortliche soll die Verzeichnisse regelmäßig überprüfen, sinnvollerweise bei Änderungen oder Neuanschaffungen, spätestens jedoch in Abständen von zwei Jahren. Bei Bedarf durch geänderte Abläufe und Organisationsstrukturen oder durch Neuanschaffung von Programmen muss die entsprechende Anpassung des Verzeichnisses von Verarbeitungstätigkeiten vorgenommen werden. In jedem Fall ist damit zu rechnen, dass im Rahmen von Prüfungen durch die Datenschutzaufsicht die Vorlage der entsprechenden Dokumentation verlangt werden wird.

7. Verarbeitung von Meldedaten in kirchlichen Rechenzentren

Eine weitere neue Regelung beinhaltet, dass die Verarbeitung von Meldedaten in kirchlichen Rechenzentren besonderen Schutzmaßnahmen zu unterziehen ist. Hintergrund sind insbesondere die Anforderungen des bundesdeutschen Gesetzgebers, der den Kirchen die Übermittlung von bestimmten Meldedaten nach dem Bundesmeldegesetz eingeräumt hat. Der Bundesgesetzgeber erwartet im Gegenzug jedoch, dass die kirchlichen Meldestellen eine hinreichende Sicherheit dafür bieten, dass mit diesen besonders sensiblen personenbezogenen Daten auch sorgfältig umgegangen wird und dass diese Daten vor unzulässigen Zugriffen besonders geschützt werden. Der Verordnungsgeber der Durchführungsverordnung hat dies berücksichtigt und die entsprechenden Anforderungen in § 8 KDG-DVO formuliert. Verwiesen wird dabei auf die Anforderungen des BSI-IT-Grundschutzkatalogs bzw. der vergleichbaren Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder auf Vorschriften, die einen vergleichbaren Schutzstandard fordern, wie etwa die in der Vorschrift genannte ISO 27001.

8. Einordnung in Datenschutzklassen

Die Einordnung der in einer Einrichtung anfallenden und zu verarbeitenden personenbezogenen Daten in die Datenschutzklassen fällt in die Zuständigkeit des Verantwortlichen. Er kann dabei die Möglichkeit der Anhörung des betrieblichen Datenschutzbeauftragten nutzen, wodurch jedoch keine Verlagerung der Zuständigkeit oder der Verantwortung erfolgt. Damit ein Verantwortlicher die Entscheidung überhaupt treffen kann, soll er eine Risikoanalyse durchführen, um sich bewusst zu werden, welche Daten und Datenübertragungswege in seiner Einrichtung anfallen und welche Sicherungen organisatorischer oder technischer Art entsprechend für den bestmöglichen Schutz zu wählen sind. Er ist dann auch dafür verantwortlich, dass die von ihm gewählten Vorgaben in der Praxis umgesetzt werden.

9. Beicht- und Seelsorgegeheimnis

Der Schutz und die Verarbeitung von Daten, welche dem Beicht- und/oder Seelsorgegeheimnis zuzuordnen sind, unterliegen gemäß § 14 KDG-DVO speziellen Anforderungen. Beichtgeheimnis und Seelsorgegeheimnis sind gemeinsam in einer Vorschrift geregelt, da staatliche Gerichte in ihren Entscheidungen häufig beide Begriffe synonym verwenden oder nur vom Seelsorgegeheimnis sprechen, wenn nach kirchlichem Verständnis eigentlich das Beichtgeheimnis gemeint ist. Damit insoweit keine Verwirrung entsteht und die gerichtlichen Entscheidungen oder Ausführungen in Kommentaren und juristi-

scher Literatur auch im Zusammenhang mit der KDG-DVO verwendet werden können, hat der Verordnungsgeber hier beide Begriffe gemeinsam in einer Regelung aufgeführt.

Es handelt sich bei den das Beicht- und/oder Seelsorgegeheimnis betreffenden Daten um besonders sensible Daten, bei denen zunächst vor allem die kirchenrechtlichen Anforderungen nach dem Codex Iuris Canonici (CIC) zu beachten sind. Aufgrund der besonderen Sensibilität dieser Daten sollten Informationen über die Beichte nicht gespeichert werden und für das erforderliche Schutzniveau mindestens die Datenschutzklasse III oder gegebenenfalls darüberhinausgehende Sicherstellungen des Schutzes dieser besonderen Daten beachtet werden.

10. Aufgaben des Verantwortlichen

10.1 Allgemeine Aufgaben

Wie auch bereits in der Vorgängerregelung ist vorgesehen, dass Einordnungen in Datenschutzklassen in Abhängigkeit der Erfordernisse für die jeweiligen personenbezogenen Daten vorgenommen werden. Der zugrundeliegende Schutzbedarf ist durch den Verantwortlichen im Rahmen einer Risikoanalyse festzustellen. Der Verordnungsgeber legt fest, dass diese Aufgabe der Zuordnung durch den Verantwortlichen vorzunehmen ist. Er muss sich die Risiken der in seinem Verantwortungsbereich verarbeiteten personenbezogenen Daten vergegenwärtigen und die geeigneten Maßnahmen treffen. Die Letztentscheidung kann - anders als die Vorarbeiten - nicht delegiert werden, insbesondere nicht auf den betrieblichen Datenschutzbeauftragten. Dieser soll in geeigneter Weise angehört werden und kann beratend einwirken.

Der Verantwortliche muss weiterhin sicherstellen, dass die aufgrund der Datenschutzklasse vorzunehmenden Sicherungsmaßnahmen auch tatsächlich beachtet und durchgeführt werden.

Neben der Risikoanalyse, welche Ausgangsbasis für die weiteren Entscheidungen ist, und der Einordnung der in der Einrichtung verarbeiteten Daten in die entsprechenden Datenschutzklassen entsprechend den Ergebnissen der vorherigen Analyse, sind die Mitarbeitenden über Gefahren und Risiken zu informieren. Der Verantwortliche muss für seinen Zuständigkeitsbereich sicherstellen, dass die von ihm entwickelten Datenschutzkonzepte und Vorgaben in der Praxis gelebt und umgesetzt werden. Weiterhin wird von ihm verlangt, dass er die von ihm für die konkreten Verarbeitungen getroffenen technischen und organisatorischen Maßnahmen, auch im Verhältnis zu den Auftrags-

verarbeitern, regelmäßig überprüft bzw. überprüfen lässt, wobei bei ihm die letztliche Gesamtverantwortung bleibt. Zwar besteht auch hier die Möglichkeit der Übertragung von Aufgaben und Befugnissen sowie der Möglichkeit von Zuarbeiten für die Entscheidungsfindung, jedoch erfolgt dadurch keine Übertragung von Verantwortlichkeit. Auch im Zusammenhang mit dem Datenschutz und der Organisation und Sicherstellung der Beachtung der datenschutzrechtlichen Anforderungen kann zwar der betriebliche Datenschutzbeauftragte unterstützend tätig werden, jedoch kann keine Übertragung von Verantwortung auf diesen vorgenommen werden. Dies schließt die Verordnung ausdrücklich aus.

Die Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz verpflichtet den Verantwortlichen in zwei Bestimmungen zur Erstellung und Umsetzung von „Konzepten":

10.2 Das Datenschutzkonzept nach der KDG-DVO

§ 16 KDG-DVO regelt die verpflichtende Erstellung eines Datensicherungskonzepts, um das Schutzziel der Verfügbarkeit nachhaltig zu unterstützen. In dem Datensicherungskonzept sollen abhängig vom Risiko des Verlustes der personenbezogenen Daten und der durch einen Verlust bedingten Auswirkungen Maßnahmen festgelegt werden, welche die dauerhafte Lesbarkeit der Daten garantieren.

Das im § 15 KDG-DVO verlangte Datenschutzkonzept geht über ein Datensicherungskonzept hinaus. Als Datenschutzkonzept wird ein Dokument bezeichnet, welches alle wichtigen Regeln beschreibt, die im Verantwortungsbereich des Verantwortlichen zum Umgang mit personenbezogenen Daten - von der Erhebung, über die Verarbeitung und Weitergabe bis hin zur Löschung bzw. Archivierung - aufgestellt wurden.

Die konkreten Maßnahmen des Datenschutzes werden im Datenschutzkonzept aus den Zielen der Einrichtung abgeleitet. In der Datenschutzleitlinie, der Präambel des Datenschutzkonzepts, wird der Stellenwert des Datenschutzes und die Umsetzungsstrategie festgelegt. Hierauf aufbauend erfolgt die Festlegung der Maßnahmen, die auch in separaten Dokumenten („Datensicherungskonzept", „Löschkonzept", „Verschlüsselungskonzept") beschrieben werden können.

11. Dienstliche und private Nutzung von dienstlichen Systemen sowie Einbringung privater Geräte

Die neue KDG-DVO befasst sich ausführlicher mit den Fragen des Einsatzes dienstlicher Geräte unter Zulassung privater Nutzung sowie des Einsatzes von Privatgeräten der Mitarbeitenden (Bring your own device). Grundsätzlich hat der Verordnungsgeber festgelegt, dass sicherzustellen ist, dass nur eine der rechtmäßigen Aufgabenerfüllung dienende Datenverarbeitung erfolgt. Dies bedingt, dass ausschließlich die vom Verantwortlichen zur Verfügung gestellten und autorisierten Programme, Geräte und Kommunikationstechnologien genutzt werden dürfen. Der Arbeitgeber stellt die Mittel seinen Mitarbeitenden vorrangig für die dienstliche Verwendung zur Verfügung. Er darf erwarten, dass diese auch ausschließlich dafür genutzt werden. Gleichermaßen muss er davon ausgehen können, dass keine weiteren Systeme oder Programme (unbefugt) von Mitarbeitenden in den dienstlichen Bereich eingebracht werden.

Der Verordnungsgeber hat durchaus gesehen, dass in kirchlichen Einrichtungen die Notwendigkeit entstehen kann, dass dennoch private Nutzungen ermöglicht werden müssen. Hierzu ist die Vorgabe getroffen worden, dass eine solche Nutzung nur ausnahmsweise erfolgen darf. Sie bedarf darüber hinaus der ausdrücklichen Zulassung durch den Verantwortlichen, der diese in schriftlicher Form erteilt. Als Inhaber der Sachmittel, die der dienstlichen Aufgabenerledigung dienen, hat der Verantwortliche auch das Recht, im Rahmen der Zulassung oder generell Vorgaben zu machen, wie mit diesen Mitteln umzugehen ist. Er darf dabei festlegen, in welchem Rahmen und unter welchen Voraussetzungen eine private Nutzung möglich ist. Je nach Bedarf und der Situation in der Einrichtung kann eine Festlegung auch in Form einer Dienstvereinbarung zwischen dem Dienstgeber und der Mitarbeitervertretung erfolgen.

Die Mitarbeitenden sollten im Blick haben, dass im Rahmen der Nutzung eine Kontrollmöglichkeit für den Dienstgeber besteht. Dieser darf sich davon überzeugen, dass die von ihm zur Verfügung gestellten dienstlichen Systeme und Sachmittel auch ausschließlich für die dienstliche Nutzung verwendet werden. Bei der Zulassung privater Nutzung besteht in gewissem Umfang ebenfalls die Möglichkeit der Kontrolle. Dies kann zunächst bedeuten, dass außergewöhnliche Aktivitäten bei der Nutzung der dienstlichen Geräte registriert werden. Der Dienstgeber darf sich und seine IT-Systeme durchaus davor schützen, dass die Mittel missbräuchlich oder gar in einem strafrechtlich relevanten Bereich genutzt werden. Verstöße fallen unter Umständen auf den Verantwortlichen zurück, so dass er sich entsprechend absichern darf. In Dienstanweisungen oder Dienst-

vereinbarungen können Voraussetzungen normiert werden, unter welchen Vorgaben eine Kontrolle zulässig ist. Bei drohenden Gefahren oder bei Verlust mobiler Geräte sollte ein Verantwortlicher immer auch die Möglichkeit einer Löschung durch Fernzugriff vorsehen. Mitarbeitende, denen die private Nutzung genehmigt worden ist, müssen dies bei der Anwendung berücksichtigen.

Gleiches gilt für den Einsatz privater Systeme im dienstlichen Umfeld. Der Verordnungsgeber erklärt diese Variante grundsätzlich für unzulässig. Auch in diesem Fall sind Ausnahmen durch den Verantwortlichen mit schriftlicher Genehmigung möglich. Der Verordnungsgeber sieht in diesem Fall vor, dass der Einsatz von Verwaltungsprogrammen für mobile Geräte (Mobile Device Management) vorgegeben und geregelt wird. Der Verantwortliche darf dem Schutz der ihm anvertrauten personenbezogenen Daten Vorrang einräumen.

Im Fall des Ausscheidens eines Mitarbeiters ist sicherzustellen, dass dienstliche Daten nach Ende der Zulassung des Einsatzes des Privatgerätes für dienstliche Zwecke datenschutzgerecht gelöscht werden.

12. Fax und E-Mail

Die KDG-DVO enthält Regelungen zum Einsatz von Faxgeräten. Die Nutzung wird in der Praxis, insbesondere im Bereich des Austauschs von Daten durch Krankenhäuser, Apotheken, niedergelassene Ärzte, Rehabilitationseinrichtungen, Altenheime, Pflegeheime und mit der Nachsorge und Betreuung der Patienten befassten Einrichtungen, für den Datenaustausch aus Sicht der Beteiligten für derzeit unausweichlich erachtet. Insofern bedurfte es einer entsprechenden Regelung in der Durchführungsverordnung.

Für den E-Mail-Verkehr enthält die KDG-DVO ebenfalls neue Anforderungen. Abhängig von der gewählten Datenschutzklasse sind geeignete Verschlüsselungsverfahren einzusetzen und/oder geschlossene und gesicherte Netzwerke zu organisieren. Im Zusammenhang mit E-Mails ist in der Einrichtung zu organisieren und zu prüfen, welche Personen Zugriffe auf die entsprechenden Postfächer haben. Es ist zu überprüfen und festzuhalten, welche Notwendigkeiten bestehen. Entsprechend sind die Zugriffsberechtigungen in geeigneter Weise zu organisieren.

13. Zeitliche Vorgaben und Ausblick

Die KDG-DVO ist in den (Erz-) Diözesen mit Wirkung zum 01. März 2019 in Kraft getreten. Zugleich sind die Vorgängerverordnungen sowie eventuell den gleichen Regelungsbereich betreffende Bestimmungen in den jeweiligen diözesanen Regelungen außer Kraft gesetzt worden.

Die KDG-DVO sieht gemäß § 27 KDG-DVO eine Verpflichtung vor, dass die Vorgaben der Verordnung unverzüglich umzusetzen sind, spätestens jedoch bis zum 31. Dezember 2019.

Der Verordnungsgeber hat festgelegt, dass die KDG-DVO innerhalb eines Zeitraums von fünf Jahren ab dem Inkrafttreten überprüft werden soll. Verordnungsgeber und Verantwortliche haben dadurch zunächst eine Planungssicherheit hinsichtlich der zu beachtenden Bestimmungen. Darüber hinaus besteht aber auch die Selbstverpflichtung, auf sich aus der Anwendung ergebende Erkenntnisse und in der Praxis festgestellte Regelungsbedürfnisse in einem überschaubaren Zeitraum zu reagieren.

Arbeitshilfe

Katholisches
Datenschutzzentrum