Kirchliches Amtsblatt
für die Erzdiözese Paderborn

Stück 12 | Paderborn, den 20. Dezember 2018 | 161. Jahrgang

Inhalt

Dokumente des Erzbischofs

Nr. 147. Beschluss der Regional-KODA Nordrhein-Westfalen vom 14. November 2018

Die Kommission zur Ordnung des diözesanen Arbeitsvertragsrechts für die (Erz-)Diözesen Aachen, Essen, Köln, Münster (nordrhein-westfälischer Teil) und Paderborn (Regional-KODA NW) hat am 14. November 2018 beschlossen:

I) Die Kirchliche Arbeits- und Vergütungsordnung (KAVO) für die (Erz-)Bistümer Aachen, Essen, Köln, Münster (nordrhein-westfälischer Teil) und Paderborn vom 15.12.1971 (KA 1971, Stück 22, Nr. 283. ff.), zuletzt geändert am 29.10.2018 (KA 2018, Stück 11, Nr. 132.), wird wie folgt geändert:

Anlage 30 zur KAVO wird wie folgt geändert:

1. In § 3 Absatz 1 wird unter dem zweiten Spiegelstrich die Datumsangabe „29. Juni 2016“ durch die Datumsangabe „2. Juli 2018“ sowie die Datumsangabe „1. Januar 2016“ durch die Datumsangabe „1. Januar 2018“ ersetzt.

2. In § 5 Absatz 2 wird ein neuer Satz 2 folgenden Wortlauts angefügt:

„Darüber hinaus findet der zwischen dem Bundesverband Deutscher Zeitungsverleger e.V. und dem Deutschen Journalisten-Verband e.V. abgeschlossene Gehaltstarifvertrag für Redakteurinnen und Redakteure an Tageszeitungen vom 2. Juli 2018 in der ab 1. Januar 2018 gültigen Fassung Anwendung.“

II) Die Änderungen unter Ziffer I) treten rückwirkend zum 1. Januar 2018 in Kraft.

Den vorstehenden Beschluss der Regional-KODA Nordrhein-Westfalen setze ich hiermit für das Erzbistum Paderborn in Kraft.

Paderborn, 29.11.2018

Der Erzbischof von Paderborn

L. S. † Hans-Josef Becker

Erzbischof

Gz.: 5/1318.20/3/44-2018

tragter für die Seelsorge in den Justizvollzugsanstalten im Erzbistum Paderborn: 19.4./1.11.2018

Beurlaubung/Freistellung

Schröder, Lukas, Vikar, unter Aufrechterhaltung der sonstigen Aufgaben zum Weiterstudium an der Theologischen Fakultät Paderborn: 3.8./1.10.2018

Todesfälle

Werner, Karl-Christoph (Magdeburg, fr. Paderborn), Pfarrer, zuletzt Pfarrer in Weißenfels, geboren 26. Juli 1952 in Zeitz, geweiht 20. Juni 1981 in Magdeburg, gestorben 12. August 2018 in Indonesien, Grab in Weißenfels

Baum, Wolfgang (Magdeburg, fr. Paderborn), Pfarrer i. R., früher Pfarrer in Gräfenhainichen, geboren 26. September 1949 in Wittenberg, geweiht 18. Juni 1983 in Magdeburg, gestorben 31. August 2018, Grab in Bad Schmiedeberg

Schmidt, Wolfgang, Geistlicher Rat Pfarrer i. R., früher Pfarrer in Schloß Neuhaus, St. Joseph und anschließend Pfarrvikar in Sürenheide, geboren 27. Dezember 1935 in Brackwede, geweiht 26. Juli 1962 in Paderborn, gestorben 3. September 2018 in Bielefeld, Grab in Brackwede (kath. Friedhof, Brackweder Str. 32, Priestergruft)

Fries, Dietmar, Pastor i. R., früher Religionslehrer an den Höheren Schulen in Geseke und Erwitte und anschließend Seelsorger in Bad Meinberg, geboren 2. Oktober 1934 in Breslau-Carlowitz, geweiht 26. Juli 1961 in Paderborn, gestorben 16. September 2018 in Detmold, Grab in Detmold-Heiligenkirchen

Hengsbach, Paul, Geistlicher Rat Pfarrer i. R., früher Pfarrer in Langenberg, geboren 28. November 1927 in Velmede, geweiht 6. August 1952 in Paderborn, gestorben 4. November 2018 in Paderborn, Grab in Langenberg (Priestergruft)

Schütte, Guido, Ständiger Diakon, zuletzt Diakon im Pastoralen Raum Pastoralverbund Bad Driburg, geboren 10. März 1964 in Ahaus/Westf., geweiht 12. März 2005 in Paderborn, gestorben 8. November 2018, Grab in Neuenheerse

Nr. 153. Aufnahme unter die Kandidaten für den Ständigen Diakonat (Admissio)

Im Auftrag des Herrn Erzbischof Hans-Josef Becker wurden durch Weihbischof Hubert Berenbrinker am 24. November 2018 in der Mutterhauskirche des Hauses Maria Immaculata zu Paderborn unter die Kandidaten für den Ständigen Diakonat aufgenommen:

Bauer, Matthias	St. Marien, Freudenberg
Kölber, Björn	St. Martin, Bigge
Krutmann, Christoph	St. Joseph, Lendringsen
Mainka, Krzysztof	St. Bruno, Soest
Major-Leonhardt, Christian	St. Patrokli, Soest
Rosenkranz, Klaus	St. Peter und Paul, Obermarsberg
Saalmann, Stefan	St. Paulus, Herford
Sandbothe, Reinhard	St. Johannes Nepomuk, Hövelhof

Nr. 154. Liturgische Beauftragungen

Im Auftrag des Herrn Erzbischof Hans-Josef Becker erteilte Herr Weihbischof Hubert Berenbrinker am 10. November 2018 in der Mutterhauskirche des Hauses Maria Immaculata zu Paderborn folgenden Kandidaten für den Ständigen Diakonat die Liturgischen Beauftragungen zum Lektorat und Akolythat:

Bozem, Mathias	St. Peter und Paul, Wormbach
Franke, Jürgen	St. Alexius, Benhausen
Kilz, Dr. Gerhard	St. Julian, Paderborn
Stallein, Lambertus	St. Johannes Baptist, Delbrück
Spiegel, Carsten	St. Laurentius, Erwitte

Bekanntmachungen des Erzbischöflichen Generalvikariates

Nr. 155. Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz für die Erzdiözese Paderborn (KDG-DVO)

Aufgrund des § 56 des Gesetzes über den Kirchlichen Datenschutz für die Erzdiözese Paderborn (KDG) vom 6. Januar 2018 (KA 2018, Nr. 23.) wird die folgende Durchführungsverordnung zum KDG (KDG-DVO) erlassen:

Inhaltsverzeichnis

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 betrieblichen Datenschutzbeauftragten, sofern ein solcher benannt wurde, vor Beginn der Verarbeitung von personenbezogenen Daten und auf entsprechende Anfrage der Datenschutzaufsicht auch dieser unverzüglich zur Verfügung zu stellen.

(2) Für bereits zum Zeitpunkt des Inkrafttretens dieser Durchführungsverordnung erfolgende Verarbeitungstätigkeiten, für die noch kein Verzeichnis von Verarbeitungstätigkeiten erstellt wurde, gilt die Übergangsfrist des § 57 Absatz 4 KDG.

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

(4) Nach den Vorschriften der Anordnung über den kirchlichen Datenschutz (KDO) bereits erstellte Verfahrensverzeichnisse sind in entsprechender Anwendung des § 57 Absatz 4 KDG den Vorgaben des § 31 KDG entsprechend bis zum 30.06.2019 anzupassen. Absatz 3 gilt entsprechend.

(5) Das Verzeichnis ist bei jeder Veränderung eines Verfahrens zu aktualisieren. Im Übrigen ist es in regelmäßigen Abständen von höchstens zwei Jahren einer Überprüfung durch den Verantwortlichen zu unterziehen und bei Bedarf zu aktualisieren. Die Überprüfung ist in geeigneter Weise zu dokumentieren (Dokumentenhistorie).

Kapitel 2
Datengeheimnis

§ 2
Belehrung und Verpflichtung auf das Datengeheimnis

(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 (Mitarbeiter im Sinne dieser Durchführungsverordnung, im Folgenden: Mitarbeiter[1]).

(2) Durch geeignete Maßnahmen sind die Mitarbeiter mit den Vorschriften des KDG sowie den anderen für ihre Tätigkeit geltenden Datenschutzvorschriften vertraut zu machen. 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. Das KDG und diese Durchführungsverordnung sowie die sonstigen Datenschutzvorschriften werden zur Einsichtnahme und etwaigen Ausleihe bereitgehalten oder elektronisch zur Verfügung gestellt; dies ist den Mitarbeitern in geeigneter Weise mitzuteilen.

(3) Ferner sind die Mitarbeiter 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 Mitarbeiter geltender Datenschutzvorschriften sowie bei Aufnahme einer neuen Tätigkeit durch den Mitarbeiter hat insoweit eine erneute Belehrung zu erfolgen.

(5) Die Mitarbeiter haben in nachweisbar dokumentierter Form eine Verpflichtungserklärung gemäß § 3 abzugeben. Diese Verpflichtungserklärung wird zu der Personalakte bzw. den Unterlagen des jeweiligen Mitarbeiters genommen. Dieser erhält eine Ausfertigung der Erklärung.

---

1 Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die gewählte männliche Form schließt eine adäquate weibliche Form gleichberechtigt mit ein.

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

§ 3
Inhalt der Verpflichtungserklärung

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

a) Angaben zur Identifizierung des Mitarbeiters (Vorname, Zuname, Beschäftigungsdienststelle, Personalnummer sowie, sofern Personalnummer nicht vorhanden, Geburtsdatum und Anschrift),

b) die Bestätigung, dass der Mitarbeiter auf die für die Ausübung seiner 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 Mitarbeiters, das KDG und andere für seine Tätigkeit geltende Datenschutzvorschriften in den jeweils geltenden Fassungen sorgfältig einzuhalten,

d) die Bestätigung, dass der Mitarbeiter über rechtliche Folgen eines Verstoßes gegen das KDG sowie gegen sonstige für die Ausübung seiner Tätigkeit spezifisch geltende Bestimmungen belehrt wurde.

(2) Die Verpflichtungserklärung ist von dem Mitarbeiter 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. Bisherige Verpflichtungserklärungen nach § 4 KDO bleiben wirksam.

Kapitel 3
Technische und organisatorische Maßnahmen

Abschnitt 1
Grundsätze und Maßnahmen

§ 4
Begriffsbestimmungen
(IT-Systeme, Lesbarkeit)

(1) IT-Systeme im Sinne dieser Durchführungsverordnung sind alle elektronischen Geräte und Softwarelösungen, mit denen personenbezogene Daten verarbeitet werden. Elektronische Geräte können als Einzelgerät oder in Verbindung mit anderen IT-Systemen (Netzwerken) bzw. anderen Systemen als Datenverarbeitungsanlage installiert sein. Softwarelösungen sind Programme, die auf elektronischen Geräten eingerichtet oder über Netzwerke abrufbar sind.

(2) Unter den Begriff „IT-Systeme" fallen insbesondere auch mobile Geräte und Datenträger (z. B. Notebooks, Smartphones, Tabletcomputer, Mobiltelefone, externe Speicher); ferner Drucker, Faxgeräte, IP-Telefone, Scanner und Multifunktionsgeräte, die Scanner-, Drucker-, Kopierer- und/oder Faxfunktionalität beinhalten.

(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 sicherzustellen, 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),

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 insbesondere folgende Maßnahmen zu treffen:

a) Unbefugten ist der Zutritt zu IT-Systemen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zutrittskontrolle).

b) Es ist zu verhindern, dass IT-Systeme von Unbefugten genutzt werden können (Zugangskontrolle).

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 un-

befugtes Auslesen, Kopieren, Verändern oder Entfernen durch geeignete Maßnahmen zu schützen.

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

f) Es ist grundsätzlich sicherzustellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in IT-Systemen verarbeitet worden sind (Eingabekontrolle). 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 Daten getrennt verarbeitet werden (Trennungsgebot).

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

(3) Absatz 2 gilt entsprechend für die Verarbeitung personenbezogener Daten in nicht automatisierter Form sowie für die Verarbeitung personenbezogener Daten außerhalb der dienstlichen Räumlichkeiten, insbesondere bei Telearbeit.

§ 7
Überprüfung

(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. 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) Insbesondere die Vorlage eines anerkannten Zertifikats gemäß § 26 Absatz 4 KDG durch den Verantwortlichen ist als Nachweis zulässig.

(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 Vorschrift 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

(1) Der Schutzbedarf personenbezogener Daten ist vom Verantwortlichen anhand einer Risikoanalyse festzustellen.

(2) 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. Hierzu zählen insbesondere die Eintrittswahrscheinlichkeit und die Schwere eines Schadens für die betroffene Person. 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) 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.

(4) 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.

(5) Die Einordnung erfolgt durch den Verantwortlichen; sie soll in der Regel bei Erstellung des Verzeichnisses von Verarbeitungstätigkeiten vorgenommen werden. Der betriebliche Datenschutzbeauftragte soll angehört werden.

(6) In begründeten Einzelfällen kann der Verantwortliche eine abweichende Einordnung vornehmen. Die Gründe sind zu dokumentieren. Erfolgt eine Einordnung in eine niedrigere Datenschutzklasse, ist zuvor der betriebliche Datenschutzbeauftragte anzuhören.

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

§ 10
Schutzniveau

(1) Die Einordnung in eine der nachfolgend genannten Datenschutzklassen erfordert die Einhaltung des dieser Datenschutzklasse entsprechenden Schutzniveaus.

(2) 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.

§ 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) Die Anmeldung am IT-System ist nur nach Eingabe eines geeigneten benutzerdefinierten Kennwortes oder unter Verwendung eines anderen, dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechenden Authentifizierungsverfahrens möglich.

c) Sicherungskopien der Datenbestände sind verschlossen aufzubewahren.

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) Die Anmeldung am IT-System ist nur nach Eingabe eines geeigneten benutzerdefinierten Kennwortes möglich, dessen Erneuerung in regelmäßigen Abständen möglichst systemseitig vorgesehen werden muss. Alternativ ist die Verwendung eines anderen, dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechenden Authentifizierungsverfahrens möglich.

b) Das Starten des IT-Systems darf nur mit dem dafür bereitgestellten Betriebssystem erfolgen.

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

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

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

§ 13
Datenschutzklasse III und Schutzniveau III

(1) Der Datenschutzklasse III unterfallen personenbezogene Daten, deren missbräuchliche Verarbeitung die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann. 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) Zum Schutz der in die Datenschutzklasse III einzuordnenden Daten ist ein Schutzniveau III zu definieren. Dieses setzt voraus, dass neben dem Schutzniveau II mindestens folgende Voraussetzungen gegeben sind:

a) 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. Das Verschlüsselungsverfahren ist dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen auszuwählen.

b) Eine langfristige Lesbarkeit der zu speichernden Daten ist sicherzustellen. 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 Beicht- oder Seelsorgegeheimnis unterliegen

(1) Personenbezogene Daten, die dem Beicht- oder Seelsorgegeheimnis unterliegen, sind in besonders hohem Maße schutzbedürftig. 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 an-

gepasste, erforderlichenfalls über das Schutzniveau der Datenschutzklasse III hinausgehende technische und organisatorische Maßnahmen ergriffen werden.

(4) 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. 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 im Rahmen einer Online-Beratung und ist insofern eine externe Anbindung unumgänglich, sind geeignete, erforderlichenfalls über das Schutzniveau der Datenschutzklasse III hinausgehende technische und organisatorische Maßnahmen 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 Mitarbeiters

§ 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 seine Mitarbeiter 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 (Datenschutzkonzept) erstellt und umgesetzt wird.

(5) 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. Bei Vorlage eines anerkannten Zertifikats durch den Auftragsverarbeiter gemäß § 29 Absatz 6 KDG kann auf eine Prüfung verzichtet werden.

(6) Der Verantwortliche kann, unbeschadet seiner Verantwortlichkeit, seine Aufgaben und Befugnisse nach dieser Durchführungsverordnung durch schriftliche Anordnung auf geeignete Mitarbeiter übertragen. Eine Übertragung auf den betrieblichen Datenschutzbeauftragten ist ausgeschlossen.

§ 16
Maßnahmen des Verantwortlichen zur Datensicherung

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

(2) Zum Schutz personenbezogener Daten vor Verlust sind regelmäßige Datensicherungen erforderlich. 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 Mitarbeiters

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

Kapitel 5
Besondere Gefahrenlagen

§ 18
Autorisierte Programme

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

§ 19
Nutzung dienstlicher IT-Systeme zu auch privaten Zwecken

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

§ 20
Nutzung privater IT-Systeme zu dienstlichen Zwecken

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

(2) 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 Mitarbeiters,

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.

Ergänzend ist dem betreffenden Mitarbeiter 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 Mitarbeitern vereinbart werden, soweit alle datenschutzrechtlichen Voraussetzungen für eine sichere Nutzung gegeben sind.

(4) Die automatische Weiterleitung dienstlicher E-Mails auf private E-Mail-Konten ist in jedem Fall unzulässig.

§ 21
Externe Zugriffe, Auftragsverarbeitung

(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. Derartige Zugriffe dürfen nur aufgrund vertraglicher Vereinbarung erfolgen. 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) 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. 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) Eine Fernwartung von IT-Systemen darf darüber hinaus nur erfolgen, wenn der Beginn aktiv seitens des Auftraggebers eingeleitet wurde und die Fernwartung systemseitig protokolliert wird.

(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.

§ 22
Verschrottung und Vernichtung von IT-Systemen, Abgabe von IT-Systemen zur weiteren Nutzung

(1) Bei der Verschrottung bzw. der Vernichtung von IT-Systemen, insbesondere Datenträgern, Faxgeräten und Druckern, sind den jeweiligen DIN-Normen entsprechende Maßnahmen zu ergreifen, die die Lesbarkeit oder Wiederherstellbarkeit der Daten zuverlässig ausschließen. 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.

§ 23
Passwortlisten der Systemverwaltung

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

§ 24
Übermittlung personenbezogener Daten per Fax

Für die Übermittlung personenbezogener Daten per Fax gilt ergänzend zu den Vorschriften der §§ 5 ff.:

(1) Faxgeräte sind so aufzustellen und einzurichten, dass Unbefugte keine Kenntnis vom Inhalt eingehender oder übertragener Nachrichten erhalten können.

(2) Sowohl die per Fax übermittelten als auch die in Sende-/Empfangsprotokollen enthaltenen personenbezogenen Daten unterliegen dem Datenschutz. Protokolle sind entsprechend sorgfältig zu behandeln.

(3) Um eine datenschutzrechtlich unzulässige Übermittlung möglichst zu verhindern, ist bei Faxgeräten, die in Kommunikationsanlagen (Telefonanlagen) eingesetzt sind, eine Anrufumleitung und -weiterschaltung auszuschließen.

(4) Daten der Datenschutzklassen II und III dürfen grundsätzlich nur unter Einhaltung zusätzlicher Sicherheitsvorkehrungen per Fax übertragen werden. So sind insbesondere mit dem Empfänger der Sendezeitpunkt und das Empfangsgerät abzustimmen, damit das Fax direkt entgegengenommen werden kann.

§ 25
Sonstige Formen der Übermittlung personenbezogener Daten

(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) Eine Übermittlung personenbezogener Daten per E-Mail an Postfächer, auf die mehr als eine Person Zugriff haben (sog. Funktionspostfächer), ist in Fällen personen-

bezogener 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.

§ 26
Kopier-/Scangeräte

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

Kapitel 6
Übergangs- und Schlussbestimmungen

§ 27
Übergangsbestimmungen

Soweit das KDG oder diese Durchführungsverordnung nicht ausdrücklich etwas anderes bestimmen, sind die Regelungen dieser Durchführungsverordnung unverzüglich, spätestens jedoch bis zum 31.12.2019 umzusetzen.

§ 28
Inkrafttreten, Außerkrafttreten, Überprüfung

(1) Diese Durchführungsverordnung tritt zum 1. März 2019 in Kraft.

(2) Zugleich treten

– die Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz für das Erzbistum Paderborn (KDD-Durchführungsverordnung – KDO-DVO) vom 13. Oktober 2015 (KA 2015, Nr. 135.),

– die Verwaltungsverordnung „Datenschutz beim Einsatz von Informationstechnik (IT-VVO)" vom 15. Juli 2005 (KA 2005, Nr. 135.),

– die Verwaltungsverordnung zur Bestimmung der zuständigen Dienststelle im Sinn von § 5 Abs. 3 Satz 1 der Verwaltungsverordnung zum Datenschutz beim Einsatz von Informationstechnik (IT-VVO) vom 25. August 2006, (KA 2006, Nr. 115.) und

– die Verwaltungsverordnung „Telefaxverkehr mit Kirchengemeinden, Gemeindeverbänden und anderen der Aufsicht des Erzbistums unterliegenden kirchlichen Institutionen" vom 11. Mai 1995 (KA 1995, Nr. 85.)

außer Kraft.

(3) Diese Durchführungsverordnung soll innerhalb von fünf Jahren ab Inkrafttreten überprüft werden.

Paderborn, den 29. November2018

L. S.

Generalvikar

Gz.: 1.7/1551/6/26-2018

Nr. 158. Verwaltungsverordnung über die Erteilung der kirchenaufsichtlichen Genehmigung bei Abschluss oder vertraglicher Änderung von Mietverträgen für Garagen und/oder Kfz-Stellplätze im nordrhein-westfälischen und im hessischen Anteil des Erzbistums Paderborn

Gemäß § 21 Absatz 2 des Gesetzes über die Verwaltung des katholischen Kirchenvermögens vom 24. Juli 1924 (GS S. 585) in Verbindung mit Artikel 7 Ziffer 3 der Geschäftsanweisung über die Verwaltung des Vermögens in den Kirchengemeinden und Gemeindeverbänden im nordrhein-westfälischen und hessischen Anteil der Erzdiözese Paderborn vom 19. Mai 1995 – Geschäftsanweisung – in der Fassung vom 29. Juli 2009 (KA 2009, Nr. 106; GV.NRW S. 818, SGV.NRW S. 2223) bedürfen Beschlüsse der Kirchenvorstände über Mietverträge,

– die unbefristet sind oder
– deren befristete Laufzeit länger als ein Jahr beträgt oder
– deren Nutzungsentgelt auf das Jahr umgerechnet 15.000,00 EUR übersteigt

zu ihrer Rechtswirksamkeit der Genehmigung durch das Erzbischöfliche Generalvikariat.

Für den Abschluss sowie die vertragliche Änderung von Mietverträgen für Garagen und/oder Kfz-Stellplätzen wird gemäß Artikel 8a der Geschäftsanweisung folgende Regelung getroffen:

§ 1
Vorausgenehmigung für den Abschluss und die vertragliche Änderung von Mietverträgen für Garagen und/oder Kfz-Stellplätze

Für Beschlüsse der Kirchenvorstände gemäß Artikel 7 Ziffer 3 der Geschäftsanweisung wird hiermit unter nachfolgenden Voraussetzungen die kirchenaufsichtliche Genehmigung erteilt:

a) der Beschluss betrifft den Abschluss oder die vertragliche Änderung von Mietverträgen über Garagen und/oder Kfz-Stellplätze, die nicht im Zusammenhang mit der Vermietung einer Wohnung oder eines Gebäudes stehen;

b) der Mietzins beträgt im Einzelfall mindestens 20,00 EUR pro Monat sowie, auf das Jahr umgerechnet, insgesamt nicht mehr als 50.000,00 EUR;

c) der Vertragsabschluss oder die vertragliche Änderung erfolgt unter Verwendung gängiger oder in Anlehnung an gängige Vertragsmuster nach aktuellem Stand, wie z. B. Haus und Grund. Das Vertragswerk enthält keine Abweichungen/Sonderabreden zu Lasten der Vermieterin;

d) der Vertrag berücksichtigt die (ab spätestens 2021 geltende) Umsatzsteuerpflicht (siehe KA 2016, Stück 4, Nr. 54. und Stück 12, Nr. 171.) bzw. einen entsprechenden Vorbehalt;

e) sowohl der jeweilige Beschluss als auch die daraus resultierenden Willenserklärungen des Kirchenvorstandes entsprechen den formalen Voraussetzungen des für die kirchliche Vermögensverwaltung geltenden staatlichen und des kirchlichen Rechts (insbesondere §§ 13, 14 S. 2 des Gesetzes über die Verwaltung des katholischen Kirchenvermögens vom 24. Juli 1924 und Art. 9 S. 1 der Geschäftsanweisung).