Oberhirtliches Verordnungsblatt

Amtsblatt für das Bistum Speyer

Herausgegeben und verlegt vom Bischöflichen Ordinariat Speyer

111. Jahrgang | Nr. 8 | 14. Dezember 2018

INHALT

Der Bischof von Speyer

256 Profanierung der Kapelle im Caritasförderzentrum St. Raphael Altleiningen

Profanierungsdekret
Az.: 2/5 – 1/18

Im Gebäudekomplex der Schlossmühle des heutigen Caritasförderzentrums St. Raphael in Alt1einingen befindet sich eine Kapelle, die am 24.12.1933 konsekriert wurde. Der Caritasverband sieht keine Möglichkeit, die dringend erforderliche Sanierung der Schlossmühle durchzuführen und hat die Absicht, das gesamte Gelände zu veräußern.

Die Kapelle wurde zuletzt während der Sommerzeit jeweils an einem Samstag im Monat für eine Vorabendmesse der heutigen Pfarrei St. Lukas, Hettenleidelheim genutzt.

Auf Antrag des Caritasverbandes und nach Anhörung des Priesterrates gemäß can. 1222 § 2 CIC sowie des Allgemeinen Geistlichen Rates und des Pfarrers der Pfarrei HI. Lukas in Hettenleidelheim ordne ich hiermit Folgendes an:

1. Die Kapelle in der Schlossmühle des Caritasförderzentrums St. Raphael in Altleiningen wird für profan erklärt. Sie verliert damit gemäß can. 1212 CIC ihre Weihe und wird auf Dauer profanem Gebrauch zugeführt.
2. Der Altar wird ebenfalls gemäß can. 1238 § 1 CIC für profan erklärt. Sofern er Reliquien enthält, sind diese zu exhumieren und an einem würdigen und sicheren Ort aufzubewahren. Ersatzweise sind sie dem bischöflichen Sekretariat zu überstellen.
3. Die Profanierung wird wirksam mit dem Ende des Profanierungsgottesdienstes, der am 27. Oktober im Rahmen der Vorabendmesse der Pfarrei HI. Lukas gefeiert wird.
4. Die liturgischen Einrichtungsgegenstände und die anderen sakralen Gegenstände müssen aus der Kirche entfernt und an einem würdigen Ort aufbewahrt werden. Sie können an einem anderen Ort ihrer Bestimmung gemäß verwendet werden entsprechend den Festlegungen im Verzeichnis des Profanierungsinventars.

Diese Urkunde wird in dreifacher Ausfertigung erstellt.

Speyer, den 27. Oktober 2018

+ Karl-Heinz Wiesemann

Dr. Karl-Heinz Wiesemann
Bischof von Speyer

257 Profanierung der Filialkirche Herz Jesu in Marnheim

Profanierungsdekret
Az.: 2/5 – 2/18

Die Filialkirche Herz Jesu in Marnheim ist wegen baulicher Schäden und damit verbundener Sicherheitsmängel nicht mehr für Gottesdienste nutzbar. Die Instandhaltung würde hohe Kosten verursachen, die in keinem sinnvollen Verhältnis zur künftig zu erwartenden Nutzung stehen. Der Verwaltungsrat der Kirchengemeinde Hl. Anna Kirchheimbolanden hat daher auf Empfehlung des Gemeindeausschusses Bolanden und des Pfarreirates der Pfarrei Hl. Anna die Aufgabe der Kirche Herz Jesu beschlossen und deren Profanierung beantragt. Nach Anhörung des Priesterrates gemäß can. 1222 § 2 CIC sowie des Allgemeinen Geistlichen Rates ordne ich daher Folgendes an:

1. Die Kirche Herz Jesu in Marnheim wird mit sofortiger Wirkung für profan erklärt. Sie verliert damit gemäß can. 1212 CIC ihre Weihe und wird auf Dauer profanem Gebrauch zugeführt.
2. Der Altar wird ebenfalls mit sofortiger Wirkung gemäß can. 1238 § 1 CIC für profan erklärt. Die Reliquie ist zu exhumieren und an einem würdigen und sicheren Ort aufzubewahren. Ersatzweise ist sie dem bischöflichen Sekretariat zu überstellen.
3. Alle liturgischen Einrichtungsgegenstände und alle anderen sakralen Gegenstände müssen vor einer profanen weiteren Verwendung des Gebäudes aus der Kirche entfernt und an einem würdigen Ort aufbewahrt werden. Sie können an einem anderen Ort ihrer Bestimmung gemäß verwendet werden entsprechend den Festlegungen im Verzeichnis des Profanierungsinventars.

Diese Urkunde wird in zweifacher Ausfertigung erstellt.

Speyer, den 7. Dezember 2018

+ Karl-Heinz Wiesemann

Dr. Karl-Heinz Wiesemann
Bischof von Speyer

258 Ordnung über die Zuwendungen an die Verbände im Bistum Speyer (ZuwendungsO-Erwachsenenverbände)

Inhalt

Präambel

Die Arbeit der Katholischen Verbände ist ein wesentlicher Baustein kirchlichen Wirkens in der Gesellschaft. Diese Verbände haben Anteil am kirchlichen Verkündigungsauftrag im Rahmen der kirchlich-hoheitlichen Gewaltausübung im Sinne des Staatskirchenrechts.

Das Bistum Speyer unterstützt daher diese Verbände auch in vielfältiger Form bei der Erfüllung von deren kirchlichem Auftrag. Die finanzielle Unterstützung seitens des Bistums wird in dieser Ordnung geregelt, die vor allem eine transparente Mittelvergabe sicherstellen soll.

§ 1
Geltungsbereich

(1) Diese Ordnung gilt für die Vergabe von Zuwendungen aus dem Diözesanvermögen an die folgend aufgelisteten katholischen Verbände im Bistum Speyer:

1. Katholische Frauengemeinschaft Deutschlands (kfd) – Diözesanverband Speyer
2. Deutsche Jugendkraft-Sportverband e.V. (DJK) – Diözesanverband Speyer
3. Kolpingwerk e.V. (Abteilung Erwachsene) – Diözesanverband Speyer

4. Katholischer Deutscher Frauenbund e.V. (KDFB) – Diözesanverband Speyer
5. Katholische Arbeitnehmerbewegung Speyer e.V. (KAB) – Diözesanverband Speyer
6. Gemeinschaft Katholischer Männer Deutschlands (GKMD)

§ 2
Personalanstellung

(1) Grundsätzlich steht es dem einzelnen Verband frei, eigenes Personal zur Erfüllung seines kirchlichen Sendungsauftrags anzustellen. Die Personalverwaltung und Gehaltsabwicklung erledigt das Bischöfliche Ordinariat. Vor der Personalauswahlentscheidung ist das Benehmen mit dem Ortsordinarius herzustellen.

(2) Sofern ein Verband von der Einstellung eigenen Personals absieht, dies aber zur Verwirklichung des kirchlichen Sendungsauftrags nötig erscheint, kann das Bistum dem einzelnen Verband im Benehmen mit dem Verbandsvorstand auch eigenes Personal zur Sicherstellung des diözesanen Auftrags im Rahmen eines sog. Drittbezogenen Personaleinsatzes zuweisen.

§ 3
Höhe der Diözesanzuwendung

(1) Den Katholischen Erwachsenenverbänden nach § 1 Abs. 1 werden in den Jahren 2019 bis 2023 jährlich insgesamt 500.000,– € zur Erfüllung ihres kirchlichen Auftrags zur Verfügung gestellt.

(2) Die Summe nach Abs. 1 verteilt sich auf die einzelnen Verbände wie folgt:

a) Die Verbände zu Ziff. 1 bis 5 erhalten jeweils einen Sockelbetrag von 50.000,– € und einen jährlichen Betrag von 247.500,– €, der gemäß der Verbands-Mitglieder am 31.12.2013 rechnerisch aufgeteilt wird.
b) Der Verband zu Ziff. 6 erhält jährlich einen Festbetrag von 2.500,– €.

(3) Die nach Abs. 2 zu errechnenden Zuwendungen werden gekürzt um Personal- und Sachaufwendungen, die das Bistum direkt für die Verbände aufbringt.

(4) Unentgeltlich werden folgende Leistungen des Bistums an die in § 1 Abs. 1 aufgeführten Verbände im Rahmen der Bischöflichen Aufsicht erbracht:

- Personalverwaltung und Gehaltsabwicklung
- Rechtsberatung
- Beratung und Begleitung durch die für die Erwachsenenverbände zuständige Organisationseinheit des Bischöflichen Ordinariates

§ 4
Grundsätzliche Zweckbindung

(1) Die Zuwendungen dürfen nur zur Bestreitung der Kosten kirchlicher Verbandsarbeit entsprechend den jeweiligen in der Verbandssatzung mit Genehmigung des Diözesanbischofs festgelegten Zwecken verwendet werden.

(2) Die Zuwendungen sind wirtschaftlich und sparsam zu verwenden.

§ 5
Antrag/Zuwendungsbescheid/Auszahlung der Zuwendungen

(1) Die Auszahlung der Zuwendungen erfolgt von Amts wegen, ohne dass es eines Antrags bedarf, jeweils zum Beginn eines Haushaltsjahres.

(2) Grundlage der Zuwendung an den einzelnen Verband ist ein schriftlicher Bescheid des Ortsordinarius, der die Gesamtzuschusssumme, die möglichen Abzüge und die Auszahlungssumme ausweist.

(3) Der Zuwendungsbescheid kann mit Nebenbestimmungen versehen werden.

§ 6
Prüfung der Verwendung

Die Verbände sind verpflichtet, jährlich den Rechenschaftsbericht einschließlich der Mitgliederentwicklung und die Jahresrechnung dem Ortsordinarius bis zum 30. Juni des Folgejahres vorzulegen. Der Ortsordinarius ist ferner jederzeit berechtigt, Bücher, Belege oder sonstige Geschäftsunterlagen anzufordern sowie die Verwendung der Zuwendung durch örtliche Erhebungen zu prüfen oder durch Beauftragte prüfen zu lassen. Der Zuwendungsempfänger hat die erforderlichen Unterlagen bereit zu halten und die notwendigen Auskünfte zu erteilen.

§ 7
Mitteilungspflichten

Der Zuwendungsempfänger ist verpflichtet, dem Ortsordinarius unverzüglich Anzeige zu erstatten, wenn:

(a) der Zuwendungszweck oder sonstige für die Bewilligung der Zuwendung maßgebliche Umstände sich ändern oder wegfallen,
(b) sich herausstellt, dass der Zuwendungszweck trotz der bewilligten Zuwendung nicht zu erreichen ist,
(c) die ausgezahlten Beträge nicht entsprechend dem Zuwendungsbescheid verwendet oder nicht mehr benötigt werden,

(d) ein Insolvenz- oder Zwangsvollstreckungsverfahren gegen ihn beantragt oder eröffnet wird,
(f) der geförderte Verband aufgelöst wird oder
(g) die Rechtsform des Verbandes sich ändert.

§ 8
Rückerstattung der Zuwendung

(1) Eine nicht ihrem Zweck entsprechende Verwendung der Zuwendung löst die Pflicht zur unverzüglichen Rückzahlung aus. Sie liegt insbesondere dann vor, wenn Gelder einem anderen Zweck als den in der Verbandssatzung festgelegtem zugeführt werden, wenn dieser unwirtschaftlich verwendet wurde, wenn der Verband aufgelöst wird oder über das Vermögen des Verbandes ein Insolvenz- oder Zwangsvollstreckungsverfahren eröffnet wird.

(2) Die Zuwendung wird zurückgefordert, wenn der Verband die Zuwendung zu Unrecht, insbesondere durch unzutreffende Angaben, erlangt hat. In diesem Fall ist die Zuwendung unabhängig davon, ob er bereits verwendet worden ist, in voller Höhe zurückzuzahlen.

(3) Die Bewilligung kann widerrufen und die Höhe der Zuwendung neu festgesetzt werden, bereits ausgezahlte Beträge können zurückgefordert oder ihre weitere Verwendung kann untersagt oder die Auszahlung weiterer Beträge kann gesperrt werden, wenn

(a) der Verband die ordnungsgemäße Mittelverwendung nicht belegen kann,
(b) sonstige im Zuwendungsbescheid enthaltene Bedingungen und Auflagen nicht eingehalten werden,
(c) die Voraussetzungen für die Bewilligung der Zuwendung sich geändert haben,
(d) der Verband durch sein Handeln gegen die Glaubens- und Sittenlehre der katholischen Kirche verstößt.

(4) Durch den Ortsordinarius festgestellte Rückzahlungsverpflichtungen sollen durch Verrechnung mit anderen Zuwendungen erfolgen.

§ 9
Schlussbestimmungen

(1) Diese Ordnung tritt am 01.01.2019 in Kraft. Mit Inkrafttreten dieser Ordnung werden die in § 1 Abs. 1 genannten Verbände aus dem Geltungsbereich der Richtlinien über die Bewilligung von Zuschüssen an kirchliche Verbände, Vereine, Stiftungen, Orden und sonstige kirchliche Rechtsträger (Zuschussrichtlinien) vom 01.09.2008 (OVB 2008, S. 137 ff) ausgenommen.

(2) Spätestens vier Jahre nach Inkrafttreten hat die verantwortliche Hauptabteilung eine Evaluation dieser Ordnung durchzuführen und dem Ortsordinarius einen darauf begründeten Vorschlag zur weiteren Regelung des Zuwendungswesens hinsichtlich der Erwachsenenverbände zu unterbreiten. Im Rahmen der Evaluation sind die betroffenen Verbände anzuhören.

(3) Diese Ordnung tritt mit Ablauf des 31.12.2023 außer Kraft und soll durch eine im Zuge der Evaluation nach Abs. 2 erstellte Neuregelung ersetzt werden.

Speyer, den 7. Dezember 2018

+ Karl-Heinz Wiesemann

Dr. Karl-Heinz Wiesemann
Bischof von Speyer

259 Gesetz über den Einsatz elektronischer Informationstechnik im Bistum Speyer (IT-Gesetz)

§ 1
Zielsetzung

Ziel dieses Gesetzes ist die Umsetzung der datenschutzrechtlichen Vorgaben in Bezug auf die elektronische Datenverarbeitung sowie die Sicherheit der elektronischen Datenverarbeitungssysteme im Bistum Speyer und seinen Kirchengemeinden.

§ 2
Geltungsbereich

(1) Dieses Gesetz gilt für die Mitarbeiterinnen und Mitarbeiter des Bistums und der Kirchengemeinden. Die hier getroffenen Weisungen sind jederzeit umzusetzen, Abweichungen davon sind nur in begründeten Ausnahmefällen möglich und bedürfen der gesonderten Genehmigung durch die Leitung der Abteilung EDV des Bischöflichen Ordinariats.

Sollten Änderungen oder Erweiterungen der Richtlinie notwendig werden, so werden diese allen Mitarbeiterinnen und Mitarbeitern bekannt gemacht.

(2) Die technischen Umsetzungsrichtlinien und Definitionen werden in einer gesonderten Durchführungsverordnung geregelt (IT-DVO).

§ 3
Kirchliches Datenschutzgesetz

Das Gesetz über den kirchlichen Datenschutz (KDG) sowie die Verordnungen zur Durchführung desselben Gesetzes bleiben von diesem Gesetz unberührt.

§ 4
Arbeitsplatzausstattung

(1) Der jeweilige Dienstgeber definiert die notwendigen Geräte und Arbeitsmittel.

(2) Die Verwendung privater Geräte und Datenträger ist zum Schutz vor elektrischen und mechanischen Beschädigungen durch die Verwendung eventuell inkompatibler Geräte und aus Gründen des Schutzes vor Schadsoftware untersagt.

(3) Nicht käuflich erworbene Geräte (bspw. Spenden und Geschenke) müssen bei der EDV-Abteilung des Bischöflichen Ordinariats gemeldet werden und dürfen erst nach Freigabe genutzt werden.

(4) Der jeweilige Dienstgeber hat dafür Sorge zu tragen, dass nur Geräte zum Einsatz kommen, die frei von Schadsoftware sind.

(5) Alle Mitarbeiterinnen und Mitarbeiter sind für den Zustand der von ihnen benutzten und der ihnen zum dienstlichen und teilweise zum privaten Gebrauch überlassenen Geräte verantwortlich. Die jeweiligen Hinweise des Herstellers zur Benutzung und soweit notwendig und verfügbar zu Pflege und Reinigung sind zu beachten.

§ 5
Auftretende Defekte und Beschädigungen

Sollten Defekte oder Beschädigungen an einem Gerät auftreten, so sind diese unverzüglich dem jeweiligen Dienstgeber zu melden. Sollte der Verdacht bestehen, dass die elektrische Betriebssicherheit eines Geräts durch eine Beschädigung gefährdet ist, so ist dieses Gerät umgehend durch den Anwender außer Betrieb zu nehmen.

§ 6
Benutzeranmeldung

(1) Die Nutzung von Arbeitsplatzrechnern ist nur mit einer ordnungsgemäßen Anmeldung erlaubt. Das Außerkraftsetzen vorhandener Sicherheitsmaßnahmen ist untersagt.

(2) Pädagogisch genutzte Rechner, wie sie zum Beispiel in Kath. Tageseinrichtungen für Kinder genutzt werden, sind keine dienstlichen Rechner.

Diese pädagogischen Rechner dürfen nicht an das Verwaltungsnetz des Dienstgebers angeschlossen werden. Die Rechner dürfen ebenfalls nicht zu dienstlichen Zwecken verwendet werden.

§ 7
Softwarenutzung

(1) Jegliche zur Tätigkeitsausübung am Arbeitsplatz benötigte Software wird durch das Bischöfliche Ordinariat nach Bedarf und vorheriger Prüfung zur Verfügung gestellt.

(2) Die Erlaubnis zur Nutzung der Software und der zur Verfügung gestellten Softwarelizenzen ist auf dienstliche Zwecke beschränkt, die Nutzung zur Ausübung einer entgeltlichen Nebentätigkeit ist untersagt.

(3) Die Installation und Nutzung von nicht durch die EDV-Abteilung des Bischöflichen Ordinariats freigegebener Software oder privater Software ist untersagt.

(4) Die Weitergabe von durch das Bischöfliche Ordinariat erworbenen Lizenzen und Softwarenutzungsrechten an Dritte ist untersagt.

§ 8
Nutzung privater Datenverarbeitungssysteme

(1) Die Nutzung privater Rechner und privater Speichermedien im Netzwerk des Dienstgebers ist untersagt.

(2) Die Verarbeitung und Speicherung dienstlicher, insbesondere personenbezogener Daten auf nicht-dienstlichen Datenverarbeitungssystemen und Speichern ist untersagt.

§ 9
Schutz vor Schadsoftware

(1) Auf allen Servern, Arbeitsplatzrechnern und Notebooks werden vom Dienstgeber aktuelle Maßnahmen zur Vermeidung von Schadsoftware getroffen.

(2) Es ist untersagt, diese Maßnahmen in Hinsicht auf deren Schutzfunktion zu ändern, zu deaktivieren, anderweitig zu manipulieren oder die Software selbst zu deinstallieren.

(3) Sollten Anzeichen dafür vorliegen, dass ein Gerät trotz aktivierter Schutzsoftware mit einem Computervirus oder ähnlicher Schadsoftware ‚infiziert' wurde, ist dies zum Schutz der auf dem jeweiligen Gerät befindlichen Daten und der anderen im Netzwerk befindlichen Geräte unverzüglich der EDV-Abteilung mitzuteilen. Bis zur Klärung durch die EDV-Abteilung ist das Gerät vom Netzwerk des Dienstgebers zu trennen.

§ 10
Verwendung der E-Mail-Adressen mit Endung „…@bistum-speyer.de“

(1) Für dienstlichen E-Mail-Verkehr ist ausschließlich der dienstliche Mail-Account zu nutzen, der durch die/den jeweilige Nutzer/in auch regelmäßig abzurufen ist.

(2) E-Mail-Adressen dürfen nur für direkte Kontakte verwendet werden und nicht für öffentliche Zwecke (newsgroups, social media, etc.) im Internet eingesetzt werden. Begründete und dringende Ausnahmefälle sind über die Leitung der EDV-Abteilung des Bischöflichen Ordinariats zu beantragen und zu genehmigen.

(3) Die Verwendung der zur Verfügung gestellten bistumseigenen E-Mail-Adressen mit der Endung „…@bistum-speyer.de“ (dienstlicher Mail-Account) ist ausschließlich auf dienstliche Zwecke beschränkt. Eine private Nutzung ist nicht gestattet. Wird eine solche E-Mail-Adresse von Dritten zur Übermittlung nicht-dienstlicher Informationen angesprochen, so sind diese umgehend zu löschen. Dem Absender ist eine private E-Mail-Adresse zu nennen.

§ 11
Verwendung des Internetzugangs am Arbeitsplatz

(1) Der am Arbeitsplatz zur Verfügung stehende Internetzugang dient der Informationsbeschaffung zu dienstlichen Zwecken.

(2) Das Herunterladen von Dateien, die potentiell mit Schadsoftware infiziert sind, in das Ordinariats-Netzwerk, auf die Festplatte des lokalen Arbeitsplatzes oder auf sonstige Speichermedien ist untersagt und kann durch die EDV-Abteilung automatisiert eingeschränkt werden.

(3) Die Liste der nicht herunterladbaren Dateitypen wird von der EDV–Abteilung festgelegt. Diese Festlegung wird regelmäßig überprüft, der aktuellen Sicherheitssituation angepasst und in der Durchführungsverordnung zu diesem Gesetz veröffentlicht.

(4) Die gelegentliche, angemessene Nutzung des Internetzugangs zur privaten Informationsbeschaffung in Pausen ist gestattet. Die Nutzung eines privaten Webmailpostfachs ist zulässig, es dürfen jedoch keinerlei Dateianhänge heruntergeladen oder geöffnet werden.

(5) Im Zusammenhang mit der gelegentlichen privaten Nutzung des Internetzugangs ist die Nutzung von Online-Angeboten mit aktiven Inhalten wie Online-Spielen, Chatrooms, anmelde- oder kostenpflichtigen Internetdiensten (Ausnahme: Webmail) sowie die Nutzung jeglicher Angebote mit erhöhter Bandbreitennutzung nicht erlaubt.

§ 12
Speicherung von Dateien im Netzwerk des Dienstgebers

(1) Die im Netzwerk des Dienstgebers verfügbaren Speicherorte dienen der sicheren und dauerhaften Speicherung erzeugter Dokumente. Auf dem Dateiserver wird zu diesem Zweck eine entsprechende Struktur angelegt, die sich nach Abteilungen bzw. Funktionsbereichen gliedert. Dateien sollen nicht redundant – also an mehreren Orten gleichzeitig – gespeichert werden, um unterschiedliche Versionsstände oder die Verwendung von veralteten Dateien zu vermeiden. Die Daten, welche auf dem Dateiserver abgelegt werden, sollen durch ein tägliches Backup gesichert werden.

(2) Wichtige Dateien dürfen nicht auf der lokalen Festplatte gespeichert werden, sondern müssen auf dem Dateiserver gespeichert werden, da dieser einem täglichen Backup unterliegt. Weiter ist es untersagt, externe Dateiserver („Clouds“) zu nutzen, sofern diese nicht von der EDV-Abteilung des Bischöflichen Ordinariats freigegeben sind. Das Nähere regelt die Durchführungsverordnung zu diesem Gesetz.

§ 13
Nutzung des Netzwerks des Dienstgebers

(1) Die Nutzung des Netzwerks des Dienstgebers und aller damit verbundenen Geräte und Dienste wie Dateiserver, Drucker, Internetzugang und Telefon darf nur mit dem persönlichen Benutzernamen und Passwort der jeweiligen Mitarbeiterin oder des jeweiligen Mitarbeiters erfolgen.

(2) Bei Verlassen des Arbeitsplatzes ist der Arbeitsplatzrechner zu sperren beziehungsweise auszuschalten.

§ 14
Nutzung von Funknetzwerken (WLAN)

(1) Es ist untersagt, eigene Geräte (Notebook, PC, Mobiltelefone) im Access Point-Modus zu betreiben und damit anderen Geräten den Zugang zum Netzwerk des Dienstgebers zu ermöglichen.

(2) Bei der Verwendung von fremden WLAN-Zugängen z.B. in Hotels ist darauf zu achten, dass die Firewall des Betriebssystems und die Schutzsoftware („Virenscanner“) aktiviert ist.

§ 15
Passwörter

(1) Grundsätzlich hat jeder Mitarbeiter selbst für die dauerhafte Sicherheit seiner Passwörter zu sorgen. Entsprechende Wechsel und die notwendige Verschwiegenheit sind hierbei unumgänglich.

(2) Alle Passwörter – persönliche als auch von mehreren Benutzern gemeinsam verwendete – sind so zu gestalten, dass diese den Festlegungen der Durchführungsverordnung zu diesem Gesetz entsprechen. Dies gilt auch dann, wenn kein entsprechender Software-Mechanismus die Einhaltung der Richtlinie erzwingt.

(3) Persönliche Kennwörter sollten zur eigenen Sicherheit und zum Schutz vor Missbrauch nie weitergegeben und auch nicht ungesichert notiert werden.

(4) Die Weitergabe von nicht personenbezogenen Passwörtern darf nur an befugte Personen erfolgen. Es ist weiterhin sicherzustellen, dass allgemeine Passwörter nur an Orten gespeichert werden, die als sicher angesehen werden können.

(5) Passwörter dürfen nicht in Passwort-Managern in Internet-Browsern gespeichert werden.

§ 16
Mobile Geräte

(1) Geräte, welche außer Haus mitgeführt werden, dürfen nicht unbeaufsichtigt gelassen werden. Ist eine dauerhafte Beaufsichtigung des Geräts nicht möglich, so sind geeignete Maßnahmen zu treffen, um einen Diebstahl möglichst effektiv zu verhindern.

(2) Passwortschutz, PIN-Abfragen und sonstige Schutzmechanismen dürfen nicht deaktiviert werden.

§ 17
Schlussbestimmungen

(1) Dieses Gesetz tritt zum 01.01.2019 in Kraft.

(2) Dieses Gesetz lässt die Rechte der Mitarbeiterinnen und Mitarbeiter aus dem Mitarbeitervertretungsrecht unberührt (§ 55 MAVO).

(3) Die Durchführungsverordnung zu diesem Gesetz erlässt der Generalvikar.

Speyer, den 7. Dezember 2018

+ Karl-Heinz Wiesemann

Dr. Karl-Heinz Wiesemann
Bischof von Speyer

Bischöfliches Ordinariat

260 Gesetz über den Einsatz elektronischer Informationstechnik im Bistum Speyer – Durchführungsverordnung (DVO-IT-Gesetz)

Aufgrund § 2 Abs. 2 des Gesetzes über den Einsatz elektronischer Informationstechnik im Bistum Speyer IT-Gesetzes werden mit Wirkung vom 01.01.2019 für das Bischöfliche Ordinariat und seine Außenstellen die folgenden Ausführungsbestimmungen getroffen.

I. Zu § 4 Abs. 1 Definition der Hardwareausstattungen

Notwendige Geräte können sein:

– Computer (Desktop-Arbeitsplatz oder Laptop)
– Drucker
– Bildschirme
– Smartphones
– zusätzliche Peripheriegeräte wie Scanner, Beamer, etc.

Ergänzend hierzu wird festgelegt:

– Alle Laptops werden zukünftig verschlüsselt.
– USB Anschlüsse werden für USB Sticks und externe Datenträger gesperrt.

Abweichende Regelungen bedürfen der expliziten Genehmigung durch die Leitung der EDV-Abteilung. In Ausnahmefällen können dienstliche USB Sticks durch die EDV-Abteilung angeschafft und freigeschaltet werden.

II. Zu § 5 – Defekte und Beschädigungen

Defekte oder Beschädigungen von EDV-Geräten sind unverzüglich der EDV-Abteilung zu melden. Dies geschieht in der Regel durch eine einfache Mail an

edv-hilfe@bistum-speyer.de.

Durch die Meldung an die obengenannte Adresse wird automatisch ein Ticket im Ticketsystem der EDV-Abteilung erstellt. Somit ist eine zeitnahe und nachvollziehbare Bearbeitung gewährleistet.

Sollte das Versenden einer Mail aufgrund des Defektes nicht mehr möglich sein, können Sie den Fehler auch telefonisch bei jedem Mitarbeiter der EDV-Abteilung melden. Das Ticket wird dann entsprechend manuell angelegt.

Bei zur Reparatur eingereichten Diensthandys nehmen die Mitarbeiter der EDV-Abteilung keinen Einblick in die privaten Daten des Mitarbeiters.

III. Zu § 6 – Benutzeranmeldung

Eine Anmeldung am Netzwerk des Bischöflichen Ordinariats darf nur mit einer ordnungsgemäßen Benutzeranmeldung erfolgen.

Eine ordnungsgemäße Anmeldung erfolgt über den Windows-Anmeldebildschirm:

Im Windows Anmeldebildschirm wird der Benutzername eingeblendet. Das einzugebende Kennwort dient zur Anmeldung an ihrem lokalen Rechner und gleichzeitig zur Anmeldung und Authentifizierung sowie der Zuteilung der Berechtigungen im Netzwerk des Bischöflichen Ordinariats. Dieses Kennwort wird deshalb auch Netzwerkkennwort genannt.

Eine Anmeldung mit einem anderen als dem eigenen Netzwerkkennwort sowie unter einem anderen, fremden Benutzernamen ist untersagt.

Ebenso untersagt ist die Umgehung der Anmeldung mit einer automatischen Anmeldung ohne Eingabe des Netzwerkkennworts.

IV. Zu § 8 Abs. 2 – Nicht dienstliche Verarbeitungssysteme

Als nicht-dienstliche Verarbeitungssysteme werden folgende Systeme definiert:

- USB-Sticks
- externe Festplatten
- private PCs und Laptops
- nicht zugelassene Cloud-Dienste (dropbox, private Cloud-Dienste, etc.)
- nicht zugelassene Messenger-Dienste (WhatsApp etc.)
- private Smartphones ohne Container-Sicherheits-Apps

Dienstliche Daten dürfen nicht dauerhaft und ausschließlich auf Laufwerk c:\ (lokales Laufwerk des Arbeitsplatzrechners) gespeichert werden. Eine Speicherung zum Zwecke eines Vortrags extern oder eines Arbeitseinsatzes außerhalb des Bischöflichen Ordinariats ist erlaubt. Im Falle eines Defekts des Arbeitsplatzrechners können diese Daten nicht wieder hergestellt werden und sind verloren.

Dienstliche Daten sind auf den entsprechenden Netzwerklaufwerken (persönlich oder Gruppe) zu speichern. Dort werden die Daten regelmäßig gesichert. Persönliche Daten sind im Laufwerk F: abzuspeichern. Dies ist ein persönliches Laufwerk, andere Mitarbeiter haben auf dieses Laufwerk keinen Zugriff (auch nicht vertretungsweise).

Dateien, welche für alle Mitarbeiter einer Gruppe beziehungsweise einer Abteilung relevant sind, müssen im Laufwerk G: gespeichert werden.

Dateien, welche abteilungsübergreifend einer bestimmten Gruppe an Mitarbeitern zugänglich sein sollen, werden in Laufwerk S: (sonstiges) gespeichert.

Hier können über die EDV-Abteilung entsprechende Ordner mit den entsprechenden Zugangsberechtigungen beantragt und eingerichtet werden.

V. Zu § 9 Abs.1 – Schutz vor Schadsoftware und Umgang mit Spam-Mails

Die vom Dienstgeber getroffenen Maßnahmen zur Abwehr von Schadsoftware und Spam-Mails basieren im Wesentlichen auf 3 Prozessen, die hier folgend als kurze Informationen dargestellt werden.

Es ist untersagt, diese 3 Maßnahmen auszuschalten bzw. zu ändern oder sonst in irgendeiner Weise zu manipulieren.

A. Firewall
Die Firewall ist ein Soft- und hardwarebasiertes System, das zwischen das Netz des Bischöflichen Ordinariats und öffentliche Netze (Internet) geschaltet wird, um den unbefugten Zugriff auf Rechner von außen zu verhindern und so interne Daten zu schützen.

B. Antivirus-Software (AV)
Ein Antivirenprogramm schützt Computer vor schädlicher Software. Diese Software ist in der Lage, bekannte Computerviren aufzuspüren, zu blockieren und gegebenfalls zu beseitigen.

C. Regelmäßige Updates
Programmfehler in Systemprogrammen (Win 7, Win 10) oder in Anwendungsprogrammen (MS Office, Acrobat-Gruppe, …) werden oft genutzt, um Schadsoftware in ein fremdes Netz einzuschleusen.

Die Hersteller der Software versuchen, durch Aktualisierungen der Software („Updates“ oder „Patches“) diese Sicherheitslücken zu schließen.

Die von den Softwareherstellern ausgelieferten Sicherheits-Updates werden von der EDV-Abteilung regelmäßig und automatisiert eingespielt.

Trotz allen Sicherheitsvorkehrungen, die diese Maßnahmen bieten, helfen diese nur beschränkt. Ein ganz geringer Bruchteil sogenannter Spam-Mails kann nicht erkannt werden und gelangt so in den Maileingang unserer Mitarbeiter.

Die Definition von Spam reicht von Werbenachrichten über illegale Angebote bis hin zu unerwünschten Massenmails jeglicher Art und kann somit auch Betrugs- oder Virenmails umfassen.

Spam-Mails stellen heutzutage ein Haupteinfallstor für Schadsoftware dar.

Umso wichtiger ist der richtige Umgang mit diesen Spam-Mails, damit das Netzwerk des Bischöflichen Ordinariats nicht mit Schadsoftware infiziert wird.

Wie sind Spam Mails zu erkennen:

Die folgenden Tipps erleichtern das Erkennen von Spam-Mails. Im Zweifel sollten Sie aber immer auch durch eigene Recherche – z. B. durch direkte Kontaktaufnahme mit dem Absender – sicherstellen, ob der Inhalt einer verdächtigen E-Mail wirklich vertrauenswürdig ist oder nicht.

1. Kennen Sie den Absender?

Manchen Spam können Sie noch vor dem Öffnen der E-Mail erkennen. Sie wissen, welche Nachrichten Sie von Ihrem E-Mail-Anbieter erhalten, welche Newsletter Sie abonniert haben, welche Online-Dienste Sie nutzen und natürlich kennen Sie auch Ihre Freunde und Bekannten. Eine E-Mail eines Ihnen völlig unbekannten Absenders sollte Ihnen daher direkt ins Auge fallen. Aber:

- Technisch versierte Spammer können den Absender einer E-Mail fälschen und sich so beispielsweise für „PayPal“, „Microsoft“ oder andere namhafte Firmen ausgeben.
- Spam kann auch von Ihnen bekannten Personen (Kollegen, etc.) stammen. Sprechen Sie den Kollegen direkt an, wenn Ihnen eine Mail ungewöhnlich vorkommt.

Spam Mails können heutzutage auch gefälschte Absenderadressen enthalten (bspw. von Kollegen) und sind oft in fehlerfreiem Deutsch geschrieben. Hier gilt besondere Achtsamkeit.

2. Ist der Betreff und der Inhalt ungewöhnlich?

Ein zusätzliches Erkennungsmerkmal neben dem Absender ist der Betreff einer E-Mail, der Ihnen Anhaltspunkte für den fragwürdigen Inhalt einer E-Mail geben kann.

Mails von Kollegen mit ungewöhnlichen Inhalten sind ebenfalls verdächtig.

3. Enthält die E-Mail drängende Handlungsaufforderungen?

Die Aufforderung, etwas in einer E-Mail unbedingt anzuklicken und persönliche Informationen preiszugeben (Bsp.: „Folgen Sie jetzt diesem Link, um Ihre Login-Informationen zu bestätigen."), ist verdächtig („Phishing"). Deshalb kann so eine drängende Aufforderung ein Merkmal für eine gefälschte E-Mail sein.

Reaktion auf Spam-Mails

- Auf Spam-Mails darf nicht reagiert werden.
- Antworten Sie nicht und leiten Sie die Mail nicht weiter.
- Klicken Sie nicht auf die Links.
- Laden Sie keine Anhänge herunter und öffnen Sie keine Anhänge.
- Spam-Mails sind direkt aus dem Posteingang und dem „Gelöscht"-Ordner zu löschen.
- Falls Sie im Zweifel sind, ob eine Mail gefälscht ist, kontaktieren Sie den Absender telefonisch oder melden Sie sich bei der EDV-Abteilung.

Mailweiterleitung

Bei Abwesenheit (Urlaub, Krankheit o.ä.) darf keine automatische Weiterleitung der Mails erfolgen. In der entsprechend eingestellten Abwesenheitsnotiz sollte lediglich einen alternative Vertretungs-Mailadresse genannt werden.

VI. Zu § 11 Abs. 3 und 5 – Verwendung des Internetzugangs

Die meisten Viren werden von ihren Opfern selbst gestartet. Viren werden in Dateiformate verpackt, die von PC-Nutzern als harmlos eingestuft werden.

Um eine unabsichtliche Aktivierung eines Virus zu verhindern, können folgende Dateiformate nicht aus dem Internet bzw. aus E-Mails heruntergeladen werden:

- .exe (ausführbare Dateien)
- .zip (komprimierte Dateiarchive)

– .bat (Befehlsfolgen zur direkten Ausführungen)
– .doc (MS-Word bis Version 2003)
– .xls (MS-Excel bis Version 2003)
– .ppt (MS-PowerPoint bis Version 2003)
– .dot (Dokumentenvorlagen MS-Office bis Version 2003)

Hinweis:

Falls Sie eine alte Version eines MS-Office Dokuments per Mail erhalten, dann bitten Sie den Absender, das Dokument in eine neue Version des Formats (.docx, .xlsx, .pptx, .dotx, ...) umzuwandeln. Dies gilt analog für Dokumente, die Sie versenden. Hier gilt: nur noch Dokumente in neuem Dateiformat versenden.

Das Umwandeln eines alten Dateiformats in das jeweils neueste Dateiformat geschieht wie folgt:

Öffnen Sie das alte Dokument in einer neuen MS-Office Version und speichern Sie das Dokument dann mit der Funktion „Speichern unter" und wählen dabei als Dateiformat das entsprechend neueste Format aus (hier „Word-Dokument")

Es wird nun eine Datei mit dem Dateiformat .docx (resp. .xlsx, .pptx) erstellt.

Streaming Dienste (youtube, Radio und Fernsehen, …)

Die Nutzung von Streaming-Diensten, die eine erhöhte Nutzung der Internet-Bandbreite benötigen, ist untersagt, kann aber für dienstliche Zwecke freigegeben werden.

Streaming-Dienste sind u.a.:

– Radio und Fernsehprogramme
– Videokanälen (youtube, etc.)

sowie die

– Synchronisierung von Clouddiensten (dropbox, icloud, etc.)

VII. Zu § 12 – Cloud- und Messenger-Dienste

Cloud-Dienste

Cloud Computing beschreibt die Bereitstellung von IT-Infrastruktur (Speicherplatz, Rechenleistung, Anwendungssoftware, etc.) als Dienstleistung über das Internet. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über Webbrowser.

Daten, welche in solchen Cloud-Diensten gespeichert werden, liegen damit außerhalb des Rechenzentrums des Bischöflichen Ordinariats.

Die dienstliche Nutzung von Cloud-Diensten, deren physikalische Datenspeicherung außerhalb des EWR und der Schweiz stattfindet, ist untersagt. Die entsprechenden Regelungen finden sich im KDG (OVB 3/2018). Dies betrifft insbesondere Dienste wie

– Dropbox
– iCloud
– Google Cloud
– etc.

Sind Sie nicht sicher, ob der von Ihnen genutzte Cloud-Dienst den gesetzlichen Anforderungen genügt, so richten Sie bitte unter it-sicherheit@bistum-speyer.de eine kurze Anfrage an die EDV des Bischöflichen Ordinariats.

Cloud-Dienste, die die formalen Anforderungen an die gesetzlichen Grundlagen des KDG erfüllen, müssen vor Nutzung durch die EDV-Abteilung geprüft und freigegeben werden.

Eine jeweils aktuelle Liste der freigegebenen Cloud-Dienste erhalten sie bei der EDV-Abteilung des Bischöflichen Ordinariats. Ihre Anfrage richten Sie bitte an it-sicherheit@bistum-speyer.de.

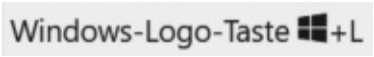
Messenger-Dienste

Die Nutzung von Messenger-Diensten wie Whatsapp, Facebook-Messenger etc. ist ebenfalls untersagt.

VIII. Zu § 13 Abs. 2 – Zugang und Sperre Arbeitsplatz

Beim Verlassen des Arbeitsplatzes ist der Rechner entweder auszuschalten (am Ende des Arbeitstages) oder der Bildschirm zu sperren, wenn die Arbeit später fortgesetzt werden soll.

Das Aktivieren der Bildschirmsperre in Windows kann mit folgender Tastenkombination durchgeführt werden:



Bei der Rückkehr zum Arbeitsplatz ist zum Entsperren des Bildschirms die Eingabe des Windows-Anmeldekennwortes erforderlich.

Beim Verlassen des leeren Büros ist die Bürotür abzuschließen. Dies gilt auch für ein kurzfristiges Verlassen des Büros.

Gewähren Sie keinen betriebsfremden Personen Zugang zu Arbeitsplatzrechnern, auch wenn diese Personen vorgeben, als Servicetechniker oder ähnliches im Auftrag der EDV-Abteilung, Kanzlei zu agieren. Halten Sie im Zweifel Rücksprache mit der EDV-Abteilung.

Anfragen nach Fernwartung durch externe Dienstleister bedürfen der Freigabe der EDV-Abteilung.

Ein selbständiges Öffnen des Fernwartungszugangs ist untersagt.

„Alte“ oder defekte Datenträger (Disketten, CD-ROMs, USB-Sticks, Festplatten usw.) dürfen nicht weggeworfen werden, sondern sind bei der EDV zur zentralen, datenschutzzertifizierten Vernichtung abzugeben.

IX. Zu § 14 Abs. 1 – WLAN

Definition Access Point Modus:

In einem WLAN ist ein Access Point (AP) eine Station, die Daten empfängt und sendet. Ein Access Point verbindet Anwender mit anderen Nutzern im Netzwerk und kann auch als Verbindungspunkt zwischen dem Funknetz und dem drahtgebundenen Netzwerk (LAN) fungieren. Vereinfacht gesprochen ist ein Access Point eine Hardware, die Nutzern per Wireless LAN Zugriff auf Netzwerkressourcen und gegebenfalls das Internet ermöglicht.

Access Points werden oft auch drahtloser Zugriffspunkt oder Basisstation genannt. Als Hotspot bezeichnet man öffentlich zugängliche Access Points.

Smartphones können im Access Point Modus betrieben werden, d. h. das Smartphone verbindet sich über das Funknetz mit dem Internet und steht gleichzeitig Anwendern in der Nähe über WLAN als zentraler Zugriffspunkt ins Internet zur Verfügung. Über das Smartphone als Zugriffspunkt kann sich bspw. ein Laptop in das Internet verbinden.

X. Zu § 15 Abs. 1 und 4 – Kennwort

Ein Kennwort dient zur Authentifizierung. Durch ein Kennwort weist sich eine Person aus und bestätigt seine eigene Identität. Neben der Rolle „Identifizieren von Personen“ werden Passwörter auch dazu verwendet, um bestimmte Berechtigungen nachzuweisen (z Bsp. auf Ordner oder auf Programme).

Das Netzwerkkennwort, welches von den Mitarbeitern des Bischöflichen Ordinariats verwendet wird, um sich am Rechner anzumelden, identifiziert den Mitarbeiter im Netzwerk des BO und ermöglicht ihm das Arbeiten im System mit den ihm zugeteilten Rechten.

Die Authentizität des sich Ausweisenden ist nur so lange sichergestellt, wie das Kennwort geheim bleibt und es Dritten nicht zugänglich ist.

Neuen Mitarbeitern wird zu Beginn der Arbeitsaufnahme durch die EDV-Abteilung ein neues Netzwerkkennwort mitgeteilt. Bei der ersten Anmeldung des Systems muss dieses Kennwort durch den Mitarbeiter auf ein persönliches Kennwort geändert werden.

Netzwerkkennwörter sind generell 12 Monate gültig. Nach Ablauf dieser Frist läuft das Systemkennwort ab und muss vom Mitarbeiter geändert werden.

Für die Neuerstellung des Kennworts gilt folgende Richtlinie:

– Das Kennwort muss mindestens 12 Zeichen lang sein.
– Im Kennwort muss mindestens ein Großbuchstabe, eine Zahl und ein Sonderzeichen enthalten sein.

Hinweise zum sicheren Umgang mit Kennwörtern:

1. Verwenden Sie möglichst komplexe Kennwörter und vermeiden Sie daher „einfache“ Kennwörter wie: ‚123456789012‘ oder sonstige fortlaufende Kennwörter und andere Muster.

Tipp:

Bilden Sie einen Satz, bei dem Sie die Anfangsbuchstaben der Wörter zum Passwort zusammensetzen.

Beispiel:

Lobe den Herren, den mächtigen König der Ehren (GL 392)

wird als Passwort zu

LdHdmKdE#392

2. Verwenden Sie beim Wechsel des Kennworts keine ähnlichen Kennwörter.

Zählen Sie beispielsweise keine Passwörter hoch und verwenden Sie keine ID’s für Zeiträume (Quartal, Jahr, etc. …).

Beispiele für nicht erlaubte Kennwortfolgen:

DOM2018	BOSP-Z1
DOM2019	BOSP-Z2
DOM2020	BOSP-Z3

3. Notieren Sie das Passwort auf keinen Fall auf Papier, Post-It's etc.

4. Speichern Sie keine Passwörter unverschlüsselt auf ihrem PC.

Um eine Vielzahl an Kennwörtern verschlüsselt auf dem PC zu speichern, gibt es entsprechende Software („Kennwort-Safe"), die dies ermöglicht.

Bei Bedarf kann diese Software von der EDV-Abteilung zur Verfügung gestellt werden.

5. Geben Sie ihre Passwörter auf keinen Fall an Dritte weiter.

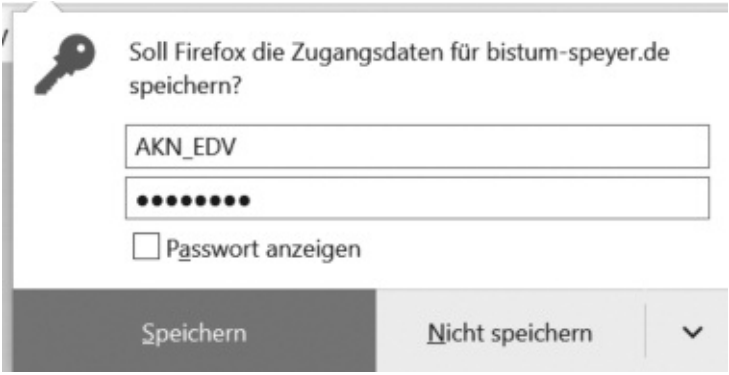
Niemand (Vorgesetze, Kollegen und EDV) hat das Recht, Ihr persönliches Passwort zu kennen.

Geben Sie Ihr Passwort auch nicht an externe Dienstleister (Techniker für Hardware; Firmen, die per Fernwartung Wartungsarbeiten auf unserem System durchführen, etc.).

6. Speichern Sie Ihr Kennwort nicht im Kennwort-Manager ihres Internet Browsers.

Der Internet Browser fragt Sie nach Eingabe eines Passworts danach, ob das Passwort für weitere Anwendungen gespeichert werden sollen.

Beispiel:



Das Kennwort darf niemals gespeichert werden. Der Kennwortmanager kann leicht ausgelesen werden und die Kennwörter missbraucht werden.

Es wird empfohlen, bereits gespeicherte Passwörter ihres Internet Browsers zu löschen.

XI. Anhang

Für weitere Anfragen in den Bereichen IT-Sicherheit und Datenschutz nutzen Sie bitte folgende spezifische E-Mailadressen:

Fragen zur IT-Sicherheit: it-sicherheit@bistum-speyer.de

Fragen zum Datenschutz: datenschutz@bistum-speyer.de

Speyer, den 7. Dezember 2018

Andreas Sturm
Generalvikar

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

in der Fassung des einstimmigen Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 19. November 2018

Aufgrund des § 56 des Gesetzes über den Kirchlichen Datenschutz (KDG) vom 2. März 2018, veröffentlicht im Oberhirtlichen Verordnungsblatt vom 22. März 2018, 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).

(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.

(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 personen-

bezogene 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 sicher zu stellen, 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 unbefugtes 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 sicher zu stellen, 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, 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 bereit gestellten 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 sicher zu stellen. 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 angepasste, 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 personenbezogener Daten der Daten-

schutzklassen 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 01.03.2019 in Kraft.

(2) Zugleich tritt die Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO – DVO) vom 9. Juni 2016 (OVB 2016, S. 140 ff) außer Kraft.

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

Speyer, den 4. Dezember 2018

Andreas Sturm
Generalvikar

262 Gestellungsgelder 2019 bis 2021

Bischof Dr. Karl-Heinz Wiesemann hat die Empfehlung der Vollversammlung des VDD übernommen und für die Diözese Speyer die Höhe der Gestellungsgelder für die Jahre 2019 bis 2021 in Kraft gesetzt.

Die Gestellungsgelder betragen somit ab dem 1. Januar 2019:

Für die Gestellungsgruppen I bis IV ergeben sich ab 1. Januar 2019 die folgenden Jahres- bzw. Monatsbeträge:

Gestellungsgruppe I:	71.300 € pro Jahr bzw.	5.940 € pro Monat
Gestellungsgruppe II:	58.800 € pro Jahr bzw.	4.900 € pro Monat
Gestellungsgruppe III:	42.900 € pro Jahr bzw.	3.575 € pro Monat
Gestellungsgruppe IV:	36.450 € pro Jahr bzw.	3.035 € pro Monat

ab 1. Januar 2020:

Gestellungsgruppe I:	73.400 € pro Jahr bzw.	6.115 € pro Monat
Gestellungsgruppe II:	60.600 € pro Jahr bzw.	5.050 € pro Monat
Gestellungsgruppe III:	44.200 € pro Jahr bzw.	3.685 € pro Monat
Gestellungsgruppe IV:	37.200 € pro Jahr bzw.	3.100 € pro Monat

ab 1. Januar 2021:

Gestellungsgruppe I:	74.200 € pro Jahr bzw.	6.185 € pro Monat
Gestellungsgruppe II:	61.200 € pro Jahr bzw.	5.100 € pro Monat
Gestellungsgruppe III:	44.700 € pro Jahr bzw.	3.725 € pro Monat
Gestellungsgruppe IV:	37.600 € pro Jahr bzw.	3.135 € pro Monat

Speyer, den 19. November 2018

Andreas Sturm
Generalvikar

263 Verfahren zur Genehmigung von Personal in Kirchengemeinden in der Diözese Speyer – Neufassung zum 1. Januar 2019

1. Genehmigung bei Aufstellung und Änderung des Stellenplans sowie bei Besetzung von Planstellen

1.1 Die Bischöfliche Finanzkammer (Referat Finanzen Kirchengemeinden) genehmigt die Stellenpläne der Kirchengemeinden der Diözese Speyer. Der Stellenplan ist die fortgeschriebene Aufstellung und zusammenfassende Darstellung der Stellen. Zum Personalstand in den

Kirchengemeinden gehören Pfarrsekretäre/Innen, Pfarrsekretäre/Innen in der Funktion Büroleitung, Organisten, alle Kirchendienstkräfte und die Beschäftigten in den Kindertagesstätten.

1.2 Die Schaffung einer neuen Stelle oder die Besetzung einer freien Stelle sowie die Erhöhung des Stellenumfangs sind schriftlich zu beantragen und durch den Verwaltungsrat zu begründen. Gleiches gilt für die Ernennung der Stelle Büroleitung in dem Zentralen Pfarrbüro. Erst nach Genehmigung der Stelle durch die Bischöfliche Finanzkammer kann die Stelle bzw. die Funktion Büroleitung besetzt werden. Dieser Punkt gilt nicht für die Beschäftigten der Kindertagesstätten.

1.3 Alle sonstigen Veränderungen von Personal (z.B. Krankheitsvertretungen, Reduzierungen von Beschäftigungsumfängen) sind der Bischöflichen Finanzkammer durch die zuständige Regionalverwaltung unverzüglich anzuzeigen.

1.4 Die Bischöfliche Finanzkammer ist – unbeschadet der Verantwortung des Verwaltungsrates – für die ständige Aktualisierung der Stellenpläne aller Kirchengemeinden in der Diözese Speyer verantwortlich.

2. Antragsverfahren

2.1 Der Antrag an das Bischöfliche Ordinariat ist vor der Besetzung bzw. Wiederbesetzung der Stelle durch die zuständige Regionalverwaltung an die Bischöfliche Finanzkammer zu richten. Dem Antrag ist ein entsprechender Beschluss des Verwaltungsrats der Kirchengemeinde beizufügen, mit Dienstsiegel und Unterschrift (siehe § 14 Kirchenvermögensverwaltungsgesetz (KVVG)).

2.2 Die Bischöfliche Finanzkammer wird den Antrag prüfen und eine entsprechende Entscheidung treffen. Eine Stelle kann im beantragten Umfang nur dann genehmigt werden, wenn die Finanzierung der Personalkosten dauerhaft und nachhaltig gesichert ist.

2.3 Die Entscheidung wird dem Verwaltungsrat durch die Bischöfliche Finanzkammer mitgeteilt. Die zuständige Regionalverwaltung, die Hauptabteilung III (Personal) und im Fall von Pfarrsekretären/Innen die Zentralstelle (Z1) erhalten einen Abdruck.

3. Arbeitsverträge und Vergütungsberechnung

3.1 Alle Arbeitsverträge und Nachträge sind durch die zuständige Regionalverwaltung der Hauptabteilung III/43 (Personal) vor Beschäftigungsbeginn zur kirchenaufsichtlichen Genehmigung vorzulegen (siehe § 17 Abs. 1 Buchstabe h) KVVG). Grundsätzlich ist die Frage der Qualifikation gemäß der internen Richtlinien zu berücksichtigen.

3.2 Arbeitsverträge sowie Änderungen von Vertragsbestandteilen, die außerhalb der genehmigten Stelle liegen, werden nicht genehmigt.

3.3 Zur Erfüllung sozialversicherungs- und steuerrechtlicher Auflagen sind sämtliche Vergütungszahlungen ausschließlich über die Hauptabteilung III/43 (Personal) – Zentrale Gehaltsabrechnungsstelle (ZGASt) vorzunehmen.

4. Inkrafttreten

Diese Neufassung tritt mit Wirkung vom 1. Januar 2019 in Kraft.

Speyer, den 30. November 2018

Andreas Sturm
Generalvikar

264 Verwaltungsvorschrift über die Bildung des ReligionslehrerInnen-Vertreterrates an berufsbildenden Schulen für die Diözese Speyer

§ 1
Geltungsbereich

Die Berufsgruppe des in der Diözese Speyer tätigen katholischen Religionslehrpersonals an Berufsbildenden Schulen wird gegenüber der Hauptabteilung II „Schulen, Hochschulen und Bildung“ durch einen Vertreterrat (VR) vertreten, der von der ReligionslehrerInnenversammlung gebildet wird. Dieser Vertreterrat ist der von der Hauptabteilung II als Partner anerkannte Sprecher des Religionslehrpersonals an Berufsbildenden Schulen in der Diözese Speyer.

§ 2
Personenbereich

Katholisches Religionslehrpersonal im Sinne dieser Satzung sind

(1) ReligionslehrerInnen im Kirchendienst
(2) ReligionslehrerInnen im Staatsdienst

welche an Berufsbildenden Schulen innerhalb des Bistums Religionsunterricht erteilen und die Wahlberechtigung zum ReligionslehrerInnen-Vertreterrat erlangt haben.

§ 3
Wahl, Amtszeit, Mitgliedschaft

(1) Wahlberechtigt und wählbar sind alle ReligionslehrerInnen gemäß § 2 Abs. 1 und 2.

(2) Eine Wahl ist auch in Abwesenheit möglich, wenn die Wahlbereitschaft schriftlich erklärt wurde.

(3) Der Vertreterrat besteht aus fünf Mitgliedern.

(4) Die Amtszeit des Vertreterrates beträgt zwei Jahre. Sie beginnt mit dem Wahltag.

(5) Die Mitgliedschaft im Vertreterrat erlischt durch
a) Ablauf der Amtszeit
b) Niederlegung des Amtes
c) Ausscheiden aus dem Schuldienst
d) Verlust der Wählbarkeit.

(6) Beratende Mitglieder sind kirchliche FachberaterInnen und staatliche FachleiterInnen.

§ 4
Vorsitz

Der Vertreterrat wählt bei seiner konstituierenden Sitzung eine/n Vorsitzende/n und eine/n Stellvertreter/in.

§ 5
Vertretungsratssitzung

Der Vertreterrat tritt zusammen:

(1) auf Einladung des/der Vorsitzenden, mindestens zweimal im Jahr

(2) auf Einladung der Hauptabteilung II „Schulen, Hochschulen und Bildung“

(3) auf schriftliches Verlangen der Mehrheit des Vertreterrats.

§ 6
Nichtöffentlichkeit und Zeit der Vertreterratssitzungen

(1) Die Sitzungen des Vertreterrats sind nicht öffentlich; sie finden außerhalb der Dienstzeit statt.

(2) Nur in begründeten Ausnahmefällen – und im Einvernehmen mit der betroffenen Schulleitung und der Hauptabteilung II – können Sitzungen des Vertreterrates während der Dienstzeit stattfinden.

§ 7
Ehrenamtliche Stellung der Mitglieder des Vertretungsrates

(1) Die Mitglieder des Vertretungsrats führen ihr Amt unentgeltlich als Ehrenamt.

(2) Versäumnis von Arbeitszeit im Sinne von § 6 Abs. 2 hat keine Minderung der Bezüge zur Folge.

§ 8
Kosten und Sachaufwand

Die durch die Tätigkeit des Vertretungsrats entstehenden Kosten trägt das Bistum Speyer – Hauptabteilung II „Schulen, Hochschulen und Bildung".

§ 9
ReligionslehrerInnenversammlung

(1) Die ReligionslehrerInnenversammlung tritt zusammen:
   a) auf Einladung des Vertretungsrats, mindestens einmal im Jahr, in der Regel bei der Jahrestagung
   b) auf Einladung der Hauptabteilung II „Schulen, Hochschulen und Bildung"
   c) auf schriftliches Ersuchen eines Drittels der ReligionslehrerInnen.

(2) Die Versammlung wird von dem/der Vorsitzenden des Vertreterrats geleitet, sie ist nicht öffentlich. Es können Sachverständige und ReligionslehrerInnen in Ausbildung eingeladen werden.

(3) Die ReligionslehrerInnenversammlung kann dem Vertreterrat Anträge unterbreiten und zu seinen Beschlüssen Stellung nehmen. Sie darf nur Angelegenheiten behandeln, die zur Zuständigkeit des Vertreterrats gehören.

§ 10
Schlussbestimmungen

Diese Verwaltungsvorschrift tritt zum 1. Dezember 2018 in Kraft. Die Satzung des ReligionslehrerInnen-Vertreterrates an berufsbildenden Schulen für die Diözese Speyer vom 1. April 1977 tritt zugleich außer Kraft.

Speyer, den 4. Dezember 2018

Andreas Sturm
Generalvikar

265 Verwaltungsvorschrift zur Wahl des Vertreterrates der ReligionslehrerInnen an Berufsbildenden Schulen

§ 1

Wahlberechtigt und wählbar sind alle ReligionslehrerInnen im Sinne der Satzung des ReligionslehrerInnen-Vertreterrates an Berufsbildenden Schulen für die Diözese Speyer.

§ 2

Die ReligionslehrerInnen wählen den Vertretungsrat; innerhalb einer Wahlperiode notwendige weitere Ersatzmitglieder werden auf der nächstfolgenden ReligionslehrerInnenversammlung gewählt.

§ 3

Der Vertretungsrat wird von den stimmberechtigten ReligionslehrerInnen in geheimer Wahl gewählt, es sei denn, eine offene Wahl wird einstimmig beantragt.

§ 4

Der jeweils amtierende Vertretungsrat trifft die Vorbereitungen zur Neuwahl und bestimmt einen Wahlausschuss, der einen Wahlvorstand ernennt.

§ 5

Die Wahl wird in der Einladung zur ReligionslehrerInnenversammlung angezeigt mit der Bitte, Wahlvorschläge zu machen.

Der Wahlausschuss veröffentlicht die Wahlvorschläge bei der ReligionslehrerInnenversammlung.

§ 6

Die stimmberechtigten Mitglieder der ReligionslehrerInnenversammlung wählen die Mitglieder des Vertretungsrates.

§ 7

(1) Das Ergebnis der Wahl wird in der Reihenfolge der Stimmenzahl vom Wahlvorstand festgestellt, bekannt gegeben und schriftlich festgehalten.

(2) Gewählt sind jene, welche die meisten Stimmen erhalten haben. Bei Stimmengleichheit findet eine Stichwahl statt.

(3) Der Wahlvorstand stellt durch Befragen fest, ob die Gewählten die Wahl annehmen. Die Zusammensetzung des Vertreterrats wird vom Wahlvorstand bekannt gegeben.

§ 8

Diese Verwaltungsvorschrift tritt zum 1. Dezember 2018 in Kraft. Die Wahlordnung des ReligionslehrerInnen-Vertreterrates an berufsbildenden Schulen für die Diözese Speyer vom 1. April 1977 tritt zugleich außer Kraft.

Speyer, den 4. Dezember 2018

Andreas Sturm
Generalvikar

266 Verbot der Vermischung von Asche und Wasser bei Austeilung des Aschenkreuzes

Nach Abschluss entsprechender labortechnischer Untersuchungen durch das LKA Baden-Württemberg wird vor möglichen, teilweise erheblich gesundheitsgefährdenden Folgen durch den Kontakt einer Mischung aus Asche und Wasser mit menschlicher Haut gewarnt.

Anlass für die Untersuchungen war das Auftreten von z. T. schweren Verätzungen bei Gottesdienstteilnehmern nach dem Auftragen des Aschenkreuzes in einem Aschermittwochsgottesdienst im Erzbistum Freiburg.

Bei der Vorbereitung und Verwendung der Asche ist sorgfältig darauf zu achten, dass eine alkalische Reaktion durch die Vermischung mit Wasser ausgeschlossen ist. Die Verwendung einer derartigen Mischung wird ausdrücklich untersagt.

267 Schriftenreihen der Deutschen Bischofskonferenz

Beim Sekretariat der Deutschen Bischofskonferenz sind folgende Broschüren erschienen:

Reihe „Verlautbarungen des Apostolischen Stuhls“

Nr. 215

Die Synodalität in Leben und Sendung der Kirche

Die Internationale Theologische Kommission hat nach Autorisierung durch den Papst ein Dokument unter dem Titel „Die Synodalität in Leben und Sendung der Kirche“ veröffentlicht.

Als „konstituierende Dimension der Kirche“, so heißt es in dem Dokument, sei die Synodalität ein Weg, der „ständig erneuert und belebt“ werden müsse, um einen „neuen missionarischen Schwung“ zu fördern, der „das gesamte Gottesvolk“ einbeziehe. Neben einer gründlichen Analyse der theologischen Bedeutung von „Synodalität“ insbesondere im Licht des Zweiten Vatikanischen Konzils will das Dokument auch Handlungsimpulse geben. Dabei betrachtet das Dokument die synodale Kirche als das Gottesvolk, „das seine Existenz als Gemeinschaft und Weggemeinschaft manifestiert und konkretisiert, indem es in der Versammlung zusammenkommt und indem alle seine Mitglieder aktiv an seinem Auftrag der Evangelisierung teilnehmen“.

Reihe „Arbeitshilfen“

Nr. 301

Schöpfungsverantwortung als kirchlicher Auftrag

Während der Herbst-Vollversammlung der Deutschen Bischofskonferenz 2017 fand ein Studientag „Schöpfungsverantwortung nach Laudato si – Umwelt und integrale Entwicklung als Aufgabe der Kirche“ statt. Als Arbeitsauftrag aus diesem Studientag wurden Handlungsempfehlungen für die Arbeit in den deutschen (Erz-)Diözesen entwickelt, die auf der Herbst-Vollversammlung 2018 verabschiedet wurden und jetzt als Arbeitshilfe vorliegen. Diese Arbeitshilfe „Schöpfungsverantwortung als kirchlicher Auftrag“ enthält zehn konkrete Empfehlungen zu Ökologie und nachhaltiger Entwicklung für die Praxis in den Bistümern. Entsprechend dem Auftrag aus Papst Franziskus Enzyklika Laudato si werden dabei Aspekte des Umweltschutzes und der integralen Entwicklung des Menschen verbunden. Die Handlungsempfehlungen berühren Angelegenheiten der Pastoral, des diözesanen Verwaltungshandelns und des gesellschaftspolitischen Engagements.

Nr. 302

Solidarität mit verfolgten und bedrängten Christen in unserer Zeit. Kuba und Venezuela

Kuba und Venezuela gehören zum katholisch geprägten Lateinamerika. Eine Benachteiligung von Christen in diesen Ländern scheint auf den ersten Blick unwahrscheinlich. Dennoch haben die Christen massive Probleme, ihren Glauben offen zu leben – zu groß sind die Einschränkungen durch die beiden autoritären politischen Systeme. Wo das Menschenrecht auf Meinungsfreiheit nicht garantiert ist, ist auch das Menschenrecht auf Religionsfreiheit bedroht. Unter solchen Bedingungen die befreiende Botschaft Jesu Christi zu verkünden, und gesellschaftliche und soziale Missstände offen zu benennen, ist ein gefährliches Wagnis. Nicht wenige, die aus ihrer christlichen Verantwortung heraus politisch aktiv werden, sind bedroht und verfolgt.

Die Arbeitshilfe gibt einen Überblick über die Situation, erläutert Konflikte, analysiert Hintergründe und lässt Mitglieder der Ortskirche zu Wort kommen. Sie richtet sich vor allem an die Gemeinden und ist zur Auslage in den Pfarreien bestimmt.

Nr. 303

Für immer zusammen. Der Bund der Ehe in Treue, Liebe und Verantwortung. Familienpastorale Arbeitshilfe zum Familiensonntag 2018/2019

Vom Sekretariat der Deutschen Bischofskonferenz wird jährlich eine pastorale Arbeitshilfe zum Familiensonntag herausgegeben. Das diesjährige Motto greift die Thematik der Ehebegleitung auf, nachdem im vergangen Jahr die Ehevorbereitung im Mittelpunkt gestanden hat.

Auch in diesem Jahr ist die Arbeitshilfe zum alleinigen Online-Gebrauch gestaltet worden. Das Online-Layout ist für die Bildschirmlesbarkeit optimiert und ein leichtes Navigieren im Text ermöglicht worden. Außerdem sind viele direkt weiterführende Internetlinks aufgenommen.

Sonstige Publikationen

Reihe „Jahresbericht Weltkirche“

Jahresbericht Weltkirche 2017

Zum achten Mal erscheint der „Jahresbericht Weltkirche“, der einen Überblick über die Vielfalt der weltkirchlichen Initiativen der katholischen Kirche in Deutschland bietet. Herausgeber ist die „Konferenz Weltkirche“, in der die weltkirchlich engagierten Einrichtungen der katholischen Kirche in Deutschland zusammenarbeiten.

Bezugshinweis

Alle genannten Veröffentlichungen können wie die bisherigen Hefte der Reihen bestellt werden beim *Sekretariat der Deutschen Bischofskonferenz, Postfach 2962, 53019 Bonn, E-Mail: broschueren@dbk.de* oder über den online-Shop der Internetseite der Deutschen Bischofskonferenz *www.dbk.de* unter dem Menüpunkt „Publikationen“. Dort können sie auch als PDF heruntergeladen werden (mit Ausnahme der Buchreihe „Forum Weltkirche“, die nur im Buchhandel zu beziehen ist). Außerdem finden sich dort auch Kurzinformationen zum Inhalt der einzelnen Broschüren.

268 Schließzeiten von Bischöflichem Ordinariat und Bischöflichem Offizialat

Am Donnerstag, dem 27. Dezember 2018, und am Freitag, dem 28. Dezember 2018, sind die Dienststellen des Bischöflichen Ordinariates einschließlich der Außenstellen geschlossen. Dies gilt auch für das Bischöfliche Offizialat.

Dienstnachrichten

Kaplansversetzung

Bischof Dr. Karl-Heinz Wiesemann hat mit Wirkung vom 1. Februar 2019 Kaplan Valentine A c h o l o n u, St. Ingbert Hl. Martin, zum Kaplan der Pfarrei Hl. Katharina von Siena Ludwigshafen ernannt.

Versetzung einer pastoralen Mitarbeiterin

Mit Wirkung vom 1. Januar 2019 wurde Pastoralreferentin Annette S c h u l z e zur Geistlichen Beraterin (Mentorin) der Pastoralreferenten/innen und Gemeindereferenten/innen in der Ausbildung mit 0,5 Stellenanteil versetzt; mit weiteren 0,5 Stellenanteil wirkt sie weiterhin in der Krankenhausseelsorge an der BG Unfallklinik in Ludwigshafen.

Entpflichtungen

Bischof Dr. Karl-Heinz Wiesemann hat mit Wirkung vom 21. Oktober 2018 Regens Markus M a g i n von seinen Aufgaben als Diözesanpräses der Kirchenchöre entpflichtet.

Des Weiteren hat er mit Wirkung vom 30. November 2018 Kaplan P. Naveen Kumar P u d o t a SCJ, Neustadt Hl. Geist, entpflichtet. Er scheidet aus dem Dienst der Diözese Speyer aus, um im Auftrag seines Ordens in Rom ein Aufbaustudium zu absolvieren.

Beilagenhinweis

1. Kirche und Gesellschaft Nr. 454

Herausgeber:	Bischöfliches Ordinariat 67343 Speyer Tel. 0 62 32 / 102-0
Verantwortlich für den Inhalt:	Generalvikar Andreas Sturm
Redaktion:	Dr. Christian Huber
Bezugspreis:	5,– € vierteljährlich
Herstellung:	Druckmedien Speyer GmbH, Heinrich-Hertz-Weg 5, 67346 Speyer

Der Text des OVB ist auf der Internetseite des Bistums Speyer *www.bistum-speyer.de* unter dem Menü „Unterstützung für Aktive / Rechtliches / Oberhirtliches Verordnungsblatt“ abrufbar.