KIRCHLICHES AMTSBLATT
FÜR DIE DIÖZESE MÜNSTER

Nr. 1 **Münster, den 1. Januar 2019** **Jahrgang CLIII**

INHALT

Verordnungen und Verlautbarungen des Bischöflichen Generalvikariates

Art. 1 Tag der Nordischen Diaspora im Bistum Münster am Sonntag, 03.02.2019

Am Sonntag, dem 3. Februar 2019 begehen wir im Bistum Münster den Tag der Nordischen Diaspora. Zu diesem Sonntag hat Sr. Anna Miriam Kaschner, cps, die Generalsekretärin der Nordischen Bischofskonferenz, folgenden Brief an die Katholiken unseres Bistums geschrieben:

Liebe Schwestern und Brüder im Bistum Münster,

zum Tag der Nordischen Diaspora ist es mir eine große Freude, Sie alle im Namen unserer Katholiken in Dänemark, Schweden, Norwegen, Finnland und Island zu grüßen.

In Nordeuropa leben derzeit rund 330.000 Katholiken, die offiziell in der katholischen Kirche gemeldet sind – die „Dunkelziffer“ dürfte aber bei rund der doppelten Anzahl liegen, da viele der katholischen Einwanderer nicht in der katholischen Kirche registriert sind.

Der prozentuale Anteil der Katholiken an der Gesamtbevölkerung liegt zwischen 0,2% in Finnland und 3% in Island. Was diese abstrakten Zahlen bedeuten, möchte ich am Beispiel Finnlands verdeutlichen: Das Bistum Helsinki, das ganz Finnland umfasst hat eine Größe, die ungefähr der Fläche der BRD entspricht. In Deutschland gibt es ca. 11.000 katholische Pfarreien und Seelsorgeverbände – in Finnland verteilen sich die wenigen Gläubigen auf ganze 7 Gemeinden.

Unter diesen Bedingungen ist katholisch-sein nicht leicht. Oft ist die nächste katholische Kirche zwei oder fünf, manchmal sogar sieben Autostunden entfernt.

Die geringe Zahl von Katholiken, die über eine so große Entfernung verteilt sind, macht die seelsorgliche Betreuung extrem schwer. Die Priester fahren im Jahr nicht selten 100.000 bis 150.000 Kilometer um die Sakramente zu spenden, den Kontakt zu den Gläubigen zu halten etc.

Die meisten Katholiken in den nordischen Ländern sind Arbeitsmigranten, die durch die Liberalisierung der Arbeitsmärkte in Europa und das große Arbeitsangebot im Norden in unsere Länder kommen – aus Polen, Kroatien, Litauen, von den Philippinen, aus Vietnam. Ein anderer Teil der Einwanderer sind Flüchtlinge: aus dem Irak, aus Syrien, aus Ruanda und dem Kongo. Wer in den nordischen Ländern die katholische Kirche erlebt, erlebt die Weltkirche mit ihrer babylonischen Sprachenvielfalt von Menschen aus mehr als 70 Nationen: Hier ist jeden Sonntag Pfingsten.

Die katholische Kirche in unseren Ländern ist eine rasant wachsende Kirche. Die Zahl der Taufen übersteigt bei weitem die Zahl der Beerdigungen. So kommt es, dass sich die Katholikenzahlen in einigen unserer Bistümer in den letzten Jahren verdrei– oder sogar vervierfacht haben.

Die Kirchensteuer wird – mit Ausnahme Schwedens –nicht vom Staat eingezogen, sondern auf freiwilliger Basis entrichtet. Viele der katholischen Einwanderer kennen keine Kirchensteuer oder sind finanziell nicht in der Lage, feste Beiträge zu entrichten. Es fehlt unseren Bistümern und Gemeinden an Kirchen, an Gemeinderäumen, an Unterrichts-Material, an Geldern für die Priesterbesoldung und an vielem mehr. Wir sind eine arme Kirche in reichen Ländern.

In Island beispielsweise erhält die katholische Kirche ein sog. „Gemeinde-Entgeltes“, das jedoch sehr gering ausfällt. Der Staat zahlt für jeden erwachsenen, registrierten Katholiken einen Beitrag von 4 Euro im Monat. Ein Gehalt für die Priester kann sich das Bistum daher nicht leisten. Es bezahlt für jeden Priester die Unterkunft und das Auto. Außerdem erhält jeder Priester 300 Euro an Geld für Verpflegung. Ohne Hilfe aus Deutschland wäre auch das nicht möglich. Doch was sind bei den hohen Lebensmittelpreisen in Island 300 Euro, wenn ein Toastbrot 4.50 Euro und eine Pizza 30 Euro kosten?

Ohne Unterstützung aus Deutschland wären auch viele Bauprojekte, die Anschaffung von Fahrzeugen, Büchern, die Förderung der theologischen Aus- und Weiterbildung von Laien, Ordensleuten und Priestern, nicht möglich. Das Ansgarwerk und hinter ihm die vielen Spender in Deutschland stehen hier für die gelebte Solidarität mit den Christen in Nordeuropa. Dafür möchte ich stellvertretend für die Katholiken in unseren Ländern ein herzliches „Vergelt’s Gott“ sagen und Sie zugleich bitten, uns auch weiterhin zu unterstützen, damit wir den Glauben auch in der Diaspora in Nordeuropa weiterhin lebendig verkünden können.

Mit herzlichen Grüssen und im Gebet verbunden.

Sr. Anna Mirijam Kaschner, cps
Generalsekretärin der
Nordischen Bischofskonferenz

Art. 2 Sitzungstermine diözesaner Gremien 2019

15. Februar	Freitag	Diözesanrat
18./19. Februar	Montag/ Dienstag	Gemeinsame Konferenz aller Räte
23. Februar	Samstag	Kirchensteuerrat
25. Februar	Montag	Diakonenrat
07. März	Donnerstag	Pfarrerkonferenz
11. Mai	Samstag	Kirchensteuerrat
14. Mai	Dienstag	Dechantenkonferenz
02./03. September	Montag/ Dienstag	Gemeinsame Konferenz aller Räte
07. September	Samstag	Kirchensteuerrat
20. September	Freitag	Diözesanrat
21. September	Samstag	Kirchensteuerrat
29. Oktober	Dienstag	Rat der Pastoralreferenten/-innen
11. November	Montag	Priesterrat
23. November	Samstag	Kirchensteuerrat
27. November	Mittwoch	Pfarrerkonferenz
29. November	Freitag	Diözesanrat

AZ: 002 6.12.18

Art. 3 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 8. Dezember 2017, veröffentlicht im Amtsblatt des Bistums Münster vom 1. Februar 2018 (KA Münster 2018, Nr. 3, Art. 45), 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.

(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.

[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.

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 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 Anonymisierun 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 vorgesehe-

nen 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 ausschlie-

ßen. 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 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 01.03.2019 in Kraft.

(2) Zugleich treten die Durchführungsverordnung zur Anordnung über den kirchlichen Datenschutz (KDO-DVO) vom 1. Oktober 2015, veröffentlicht im Amtsblatt des Bistums Münster vom 15. Oktober 2015 (KA Münster 2015, Nr. 19/20, Art. 187) und die Ausführungsbestimmungen zum Datenschutz beim Einsatz von Informationstechnik vom 1. September 2005, veröffentlicht im Amtsblatt des Bistums Münster vom 1. Oktober 2005 (KA Münster 2005, Nr. 19, Art. 219) außer Kraft.

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

Münster, 4. Dezember 2018

Dr. Klaus Winterkamp
Generalvikar

Art. 4

Richtlinien des Bischöflichen Generalvikariates für die Förderung zur Familienzusammenführung für schutzberechtigte Flüchtlinge

Präambel

Die katholische Kirche und ihre Caritas im Bistum Münster setzen sich für den Schutz der Familie und das Recht auf Familiennachzug für schutzberechtigte Flüchtlinge ein. Zum Welttag der Migranten im Jahr 2018 schlug der Papst 21 Maßnahmen für eine Neuausrichtung der Flüchtlingspolitik vor. U.a. setzt er sich ein für eine Förderung der Familienzusammenführung - einschließlich Großeltern, Geschwistern und Enkelkindern – „ohne Rücksicht auf deren wirtschaftliche Kapazitäten“.

Die Familienzusammenführung wird auch schon durch einige Verbände und Gemeinden durch finanzielle Zuschüsse praktisch unterstützt. Pastorale und pädagogische Mitarbeitende sowie Ehrenamtliche in Pfarreien, Ehrenamtsgruppen, Beratungsstellen und Jugendhilfeeinrichtungen im Bistum Münster erhalten Anfragen von Hilfesuchenden zum finanziellen Zuschuss zur Familienzusammenführung. Da es bis dato auf Diözesanebene keine Regelung zur Förderung von Familienzusammenführung gibt, suchen Fachkräfte und Ansprechpersonen vor Ort in jedem Einzelfall eine individuelle Unterstützungsmöglichkeit. Dies führt dazu, dass die Höhe der Zuschüsse vor Ort teils erheblich variiert, bis dahin, dass in einigen Fällen keine Förderung erbracht wird. Nicht selten geraten Geflüchtete in Situationen existenzieller Verschuldung, um ihre Familienzusammenführung zu finanzieren. Eine bistumsweite Regelung zum Zuschuss der Familienzusammenführung schafft Kontinuität und Transparenz für Asylberechtigte ebenso wie für Ansprechpersonen vor Ort.

1. Zielsetzung / Geltungsbereich

   Diese Richtlinie regelt die Voraussetzungen, unter denen eine Auszahlung von Fördermitteln des Bistums Münster an kirchliche Einrichtungen möglich ist. Dazu zählt die finanzielle Unterstützung für Schutzberechtigte im Rahmen der Familienzusammenführung sowie die Entlastung der Ansprechpersonen vor Ort durch die Schaffung einer sog. Drittellösung. Ein Rechtsanspruch auf eine Zuwendung wird durch diese Richtlinie nicht begründet.

   Der Geltungsbereich dieser Richtlinie entspricht grundsätzlich § 1 HKO.

2. Zuwendungsvoraussetzungen

   Antragsberechtigt gelten Personen, wenn folgende Voraussetzungen erfüllt werden:

   2.1. Die begünstigte Person muss als Flüchtling anerkannt oder asylberechtigt sein oder einen anderen humanitären Aufenthaltstitel haben.

   2.2 Die begünstigte Person muss ihren Wohnsitz im NRW-Teil des Bistums Münster haben und von einem Fachdienst für Integration und Migration (FIM) der örtlichen Caritas- und Fachverbände beraten werden.

   2.3 Die Ausländerbehörde muss der Familienzusammenführung zugestimmt haben bzw. es muss eine behördliche Einreiseerlaubnis vorliegen.

   2.4 Die materielle Situation der Familie muss die Erfordernis einer finanziellen Unterstützung notwendig machen.

   2.5 Die Familienzusammenführung findet zeitnah statt oder hat vor kurzer Zeit stattgefunden, d. h. zwischen der Einreise und dem Antragseingang liegen maximal drei Monate.

   2.6 Es wird ein Zuschuss ausschließlich zu den Reisekosten im Rahmen der Familienzusammenführung gewährt. Weitere Auslagen im Rahmen der Familienzusammenführung wie Visagebühren und Übernachtungskosten werden nicht berücksichtigt. Bei dem Zuschuss handelt es sich um privilegiertes Einkommen nach § 11a Absatz 4 SGB II. Der Zuschuss wird einmalig erbracht und dient allein der Bezuschussung der Reisekosten.

3. Umfang, Höhe und Art der gewährten Zuwendungen

   3.1. Drittelung der Reisekosten

   3.1.1 Ortsebene

   Ein Drittel der Reisekosten wird auf Ortsebene sichergestellt. Anteilig kann dies durch Zuschüsse der Kirchengemeinde, des örtlichen Caritas- oder Fachverbandes und durch die antragstellende Person sichergestellt werden.Es empfiehlt sich, zwischen den Akteuren vor Ort möglichst Vereinbarungen über den Einzelfall hinaus zu treffen.

3.1.2 Katholische Arbeitsgemeinschaft Migration Ein Drittel der Reisekosten wird auf Antrag - soweit Fördermittel zur Verfügung stehen - von der katholischen Arbeitsgemeinschaft Migration (KAM) mit Sitz in Freiburg bezuschusst.

3.1.3 Bistum Münster

Das Bistum Münster bezuschusst im Rahmen der zur Verfügung stehenden Haushaltsmittel und auf Antrag ein Drittel der Reisekosten, um Familienzusammenführungen zu Schutzberechtigten zu ermöglichen. Stehen KAM-Mittel punktuell nicht zur Verfügung, bezuschusst das Bistum Münster zwei Drittel der Reisekosten.

4. Antrags- und Bewilligungsverfahren

Grundlage für den Zuschuss zur Familienzusammenführung durch das Bistum Münster sind das vollständig ausgefüllte Formblatt „Zuschuss zur Familienzusammenführung – Antragsformular für Caritas-Beratungsstellen“ der KAM sowie das Beiblatt „Zuschuss zur Familienzusammenführung durch das Bistum Münster“. Der FIM reicht sowohl das Formblatt der KAM als auch das Beiblatt des Bistums Münster beim Caritasverband für die Diözese Münster e.V. ein.

4.1 Dem örtlichen Fachdienst für Integration und Migration obliegt

4.1.1 die Unterstützung der antragstellenden Person bei der Organisation der Familienzusammenführung. Dies beinhaltet auch einen kostenbewussten Umgang mit Reisezuschüssen die Sicherstellung der Finanzierung eines Drittels der Reisekosten durch Akteure vor Ort.

4.1.2. die Vorleistung für 1/3 KAM-Mittel

4.1.3 die Auszahlung der Zuschüsse an die antragstellende Person.

4.2. Dem Caritasverband für die Diözese Münster e.V. obliegt

4.2.1 die Beratung der FIM zum Bistumsfonds für Familienzusammenführung, die inhaltliche Prüfung sowie die Befürwortung der Anträge für das Bistum Münster.

4.2.2 die Prüfung, ob zum Zeitpunkt der Antragstellung KAM-Mittel zur Verfügung stehen. Ist dies der Fall, wird das Formblatt „Zuschuss“ an die KAM und das Beiblatt an das Bistum Münster zwecks Bewilligung weitergeleitet.

Stehen punktuell keine KAM-Zuschüsse zur Verfügung, leitet der DiCV Münster sowohl das Formblatt als auch das Beiblatt an das Bistum Münster weiter mit Bitte um Förderung von zwei Drittel der Reisekosten.

4.3 Dem Bischöflichen Generalvikariat obliegt

4.3.1 die Bewilligung und Zuweisung der Mittel.

5. Verwendungsnachweis

5.1. Nach Abschluss des Verfahrens der Familienzusammenführung hat der verantwortliche Fachdienst für Integration und Migration einen Verwendungsnachweis in vereinfachter Form zu erstellen. Alle im Zusammenhang mit dieser Bewilligung stehenden Belege sind dem örtlichen Caritas- oder Fachverband vorzulegen und aufzubewahren. Hierzu ist der beigefügte Vordruck zu verwenden. Dieser Nachweis ist zu den Buchungsunterlagen zu nehmen.

Die Prüfung der Verwendung der Mittel erfolgt gemäß §§ 71 und 72 der HKO bzw. gemäß den Allgemeinen Bewilligungsbedingungen für den nordrhein-westfälischen Teil des Bistums Münster.

6. Inkrafttreten

Diese Richtlinien treten am 01.11.2018 in Kraft.

Münster, 30.10.2018

Dr. Klaus Winterkamp
Generalvikar

Vereinfachter Verwendungsnachweis gem. Ziffer 5.1 der Richtlinien für die Förderung zur Familienzusammenführung für schutzberechtigte Flüchtlinge

Verband / Einrichtung : _____

Ort: _____

Bewilligungsbescheid vom: _____

Gefördertes Projekt:

Sachbericht (Kurzdarstellung der durchgeführten Maßnahme):

Die gewährte Zuwendung in Form eines Zuschusses des oben genannten Bewilligungsbescheides in Höhe von _____ Euro wurde den Bewilligungsbedingungen entsprechend verwendet.
Die dem Bewilligungsbescheid zugrunde liegende Projektkalkulation wurde eingehalten.

Aufgestellt und sachlich richtig*: _____
Datum / Rechtsverbindliche Unterschrift Verband / Einrichtung

**Die Verwaltung der Mittel obliegt der für die Durchführung der Flüchtlingsarbeit verantwortlichen Stelle.*

Beiblatt

Richtlinien des Bischöflichen Generalvikariates für die Förderung zur Familienzusammenführung für schutzberechtigte Flüchtlinge vom 30.10.2018

Gemäß der o.g. Richtlinie beantragen wir einen Zuschuss für die Familienzusammenführung zu _____ (Name, Vorname), wohnhaft in _____ (Ort).

Der Antrag „Zuschuss zur Familienzusammenführung“ der Katholischen Arbeitsgemeinschaft Migration (KAM) ist vollständig ausgefüllt und diesem Beiblatt beigefügt.

Beantragende Einrichtung/Fachdienst für Integration und Migration
Kontaktdaten

_____
_____
_____
_____
_____
_____

Die Richtigkeit der Angaben wurde geprüft.

_____ _____
Ort, Datum Unterschrift der Bearbeiterin/des Bearbeiters
und Stempel der Einrichtung

.....

AUSZUFÜLLEN VOM CARITASVERBAND FÜR DIE DIÖZESE MÜNSTER E.V.

Zuschüsse der Katholischen Arbeitsgemeinschaft Migration stehen zur Verfügung.
☐ Ja ☐ Nein

Der Antrag ist geprüft, entspricht der Richtlinie und soll bewilligt werden.
Wir bitten um einen Zuschussbetrag in Höhe von _____ EUR.

Der Antrag wird nicht befürwortet, weil_____
_____

_____ _____
Ort, Datum Unterschrift der Bearbeiterin/des Bearbeiters

.....

VERMERK BGV MÜNSTER

_____
_____
_____

Art. 5 **Exerzitien für Priester und Diakone in der Benediktinerabtei Weltenburg**

Termin: 25. - 29. März 2019
17.30 Uhr - ca. 9.00 Uhr
Thema: „Katholische Spiritualität im Zeitalter der Ökumene“ - Schweigeexerzitien für Priester und Diakone
Leitung: Prof. Dr. Ludwig Mödl, München

Termin: 7. - 11. Oktober 2019
17.30 Uhr - ca. 9.00 Uhr
Thema: „Ich suche dich, Du Unbegreiflicher“ - Die Rede von Gott als Zentrum christlicher Verkündigung - Schweigeexerzitien für Priester und Diakone
Leitung: Prof. Dr. Ludwig Mödl, München

Termin: 11. - 16. November 2019
17.30 Uhr - ca. 9.00 Uhr
Thema: „Was ist das Menschlein, dass du seiner gedenkst?! (Psalm 8,5) Menschliche Existenz - zwischen Scheitern und Leben im Licht - Schweigeexerzitien für Priester und Diakone
Leitung: Dr. Wilfried Hagemann, Münster

Auskunft und Anmeldungen: Benediktinerabtei Weltenburg, Haus St. Georg, 93309 Weltenburg, Tel.: 09441/6757-500, Fax: 09441/6757-537

Art. 6 **Warnung**

Im Auftrag der Glaubenskongregation gibt Erzbischof Dr. Nikola Eterovic zur Kenntnis, dass ein gewisser Herr Hilary Aboh Ogochukw, ehemals Priester der Erzdiözese Bertoua in Kamerun, mit Dekret des Heiligen Vaters vom 3. Mai 2013, das von ihm gemäß can. 56 CIC im Juni 2014 zur Kenntnis genommen wurde, aus dem Klerikerstand aufgrund sexuellen Missbrauchs an Minderjährigen und Erwachsenen entlassen wurde.

Dem Apostolischen Nuntius in Karnerun wurde in einem Brief eines afrikanischen Priesterstudenten in Frankfurt a.M. zur Kenntnis gebracht, dass der Genannte im Erzbistum Köln u. a. in der französischsprachigen Mission priesterlich wirkt und ungültig die Sakramente spendet.

Der seit Juni 2014 wegen sexuellen Missbrauchs an Minderjährigen und Erwachsenen aus dem Klerikerstand entlassene ehemalige Priester Hilary Aboh Ogochukuwu stellt eine Gefahr fiir Kinder und Jugendliche dar.

AZ: PA S 2173/18 10.12.18

Art. 7 **Veröffentlichung freier Stellen für Priester und Pastoralreferentinnen/ Pastoralreferenten**

Detailinformationen zu den einzelnen Stellen sind in der Hauptabteilung 500, Seelsorge-Personal zu erhalten. Die Veröffentlichungen erscheinen ebenfalls im Internet unter ‚www.bistum-muenster.de/Stellenbekanntgabe’. Hier finden Sie auch einen Rückmeldebogen, über den Sie Ihr Interesse bekunden können.

Weitere Auskünfte erteilen je nach Angabe:

- Karl Render, Telefon: 0251 495-1304, E-Mail: render@bistum-muenster.de
- Maria Bubenitschek, Telefon: 0251 495-1304, E-Mail: bubenitschek@bistum-muenster.de
- Offizialatsrat Msgr. Bernd Winter, Telefon: 04441 872-281, E-Mail: bernd.winter@bmo-vechta.de

Folgende Stellen sind zu besetzen:

Stellen für Pfarrer

Bischöflich Münstersches Offizialat		**Auskünfte erteilt**
Dekanat Vechta	**Bakum** St. Johannes Baptist	Offizialatsrat Msgr. Bernd Winter

AZ: HA 500 1.1.19

Art. 8 **Personalveränderungen**

G ö b e l, Frank, zum 1. Juli 2019 als Pastoralreferent in der Kirchengemeinde Rheine St. Dionysius.

H ü w e, Thomas, zusätzlich zu seinen Aufgaben als Pfarrer in Rheine St. Johannes der Täufer zum Dechanten im Dekanat Rheine für die Zeit vom 1. Januar 2019 bis zum 31. Dezember 2025 ernannt.

K n o p, Thorsten, Ständiger Diakon (mit Zivilberuf) in Haltern am See St. Sixtus zum 1. Januar 2019 in der Pfarrei Dülmen St. Viktor.

K ö n i g, Franziska, zum 1. Januar 2019 mit 50 % als Mitarbeiterin im pastoralen Dienst in der Jugendkirche effata(!).

P a r a c i e j, Andrzej, zum 1. Dezember 2018 zum Kaplan in der Polnischen Katholischen Mission im Offizialatsbezirk Oldenburg ernannt.

S w i a t e k, Tomasz, mit Ablauf des 30. November 2018 als Pastor m. d. T. Pfarrer in der Polnischen Katholischen Mission im Offizialatsbezirk Oldenburg entpflichtet.

T h e b e n, Gerhard, weiterhin zum Diözesanfrauenseelsorger und zum Diözesanpräses der Kath. Frauengemeinschaft Deutschlands – kfd-Diözesanverband Münster e. V. ernannt. Er bleibt weiterhin Spiritual der Clemensschwestern in Münster.

T h o m a s, Bibin, zum Kaplan in Wilhelmshaven St. Willehad ernannt.

W e i d e m a n n, Norbert, mit Ablauf des 13. Dezember 2018 von seinen Aufgaben in der Krankenhausseelsorge in Vreden entpflichtet. Zugleich wurde er zum 15. Dezember 2018 zum Pastor m. d. T. Pfarrer in Vreden St. Georg ernannt.

Es wurde emeritiert:

E r n s t, Gerhard, von seinen Aufgaben in Münster Heilig Kreuz und Havixbeck St. Dionysius und St. Georg entpflichtet. Zum 1. Januar 2019 den Status eines parochus emeritus verliehen.

L u b e, Günther, mit Wirkung vom 1. Februar 2019 von seinen Aufgaben als Pastor m. d. T. Pfarrer in Ascheberg St. Lambertus, Landesbezirkspräses der Historischen Schützenbruderschaften Westfalen, Bezirkspräses der Deutschen Schützenbruderschaften der Region Warendorf und Diözesanpräses der Historischen Deutschen Schützenbruderschaften im Bistum Münster entpflichtet und zugleich den Status eines parochus emeritus verliehen.

T h i e d e, Christian, Dr., zum 1. Mai 2019 in den kirchlichen Ruhestand versetzt.

AZ: HA 500 1.1.19

Art. 9 **Unsere Toten**

F r i n t r o p, Dieter, Pfarrer em., geboren am 14. Februar 1935 in Münster, zum Priester geweiht am 29. Juni 1962 in Münster. Nach seiner Priesterweihe war er zunächst als Kaplan in Greven St. Martinus tätig. Im Jahr 1965 wurde er Kaplan in Hamm (Heessen) St. Stephanus. Ein Jahr darauf wurde er Kaplan in Neuenkirchen St. Anna. 1970 übernahm er die Aufgaben als Religionslehrer an den Kaufmännischen Unterrichtsanstalten des Kreises Beckum in Ahlen und als Subsidiar an St. Gottfried. Im Jahr 1972 wurde er zum Berufsschulpfarrer ernannt. Die Ernennung als Pfarrer in Coesfeld St. Jakobi und zum Definitor im Dekanat Coesfeld erfolgte 1976. Im darauffolgenden Jahr wurde er Leiter des Pfarrverbandes Coesfeld und 2000 Vicarius Cooperator m. d. T. Pfarrer im damaligen Pfarrverband Coesfeld. Seit 2007 lebte und wirkte er als Pfarrer Emeritus in Coesfeld St. Lamberti und engagierte sich weiterhin als Seelsorger in der JVA Coesfeld und im Altenheim St. Katharinenstift.

AZ: HA 500 1.1.19

Verordnungen und Verlautbarungen des Bischöflich Münsterschen Offizialates in Vechta

Art. 10 **Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO)**

Aufgrund des § 56 des Gesetzes über den Kirchlichen Datenschutz (KDG) vom 25.04.2018, veröffentlicht im Amtsblatt des Bistums Münster vom 15. Mai 2018 (KA Münster 2018, Nr. 9/10, Art. 125), setze ich hiermit die Durchführungsverordnung zum KDG (KDG-DVO) in der Fassung des einstimmigen Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 19. November 2018 für den Oldenburgischen Teil der Diözese Münster mit folgender Änderung zum 01.03.2019 in Kraft:

Es gilt die Durchführungsverordnung zum KDG (KDG-DVO), die im Amtsblatt des Bistums Münster vom 1. Januar 2019 Nr. 1 Art. 3 abgedruckt ist, mit Änderung in § 28:

„§ 28

Inkrafttreten, Außerkrafttreten, Überprüfung

(1) Diese Durchführungsverordnung tritt zum 01.03.2019 in Kraft.

(2) Zugleich tritt die Durchführungsverordnung zur Anordnung über den kirchlichen Datenschutz (KDO-DVO) vom 30.10.2015, veröffentlicht im Amtsblatt des Bistums Münster vom 01.12.2015 (KA Münster 2015, Nr. 23. Art. 240) außer Kraft.

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

Vechta, 17.12.18

L.S: + Wilfried Theising
Bischöflicher Offizial und
Weihbischof

KIRCHLICHES AMTSBLATT
FÜR DIE DIÖZESE MÜNSTER
PVS Deutsche Post AG
Entgelt bezahlt, H 7630
Bischöfliches Generalvikariat
Hauptabteilung 100
Postfach 1366, 48135 Münster

Der laufende Bezug des Kirchlichen Amtsblattes erfolgt durch die Druckerei Joh. Burlage, Kiesekampweg 2, 48157 Münster. Neubestellungen sind an das Bischöfliche Generalvikariat, 48135 Münster, Abbestellungen bzw. Ummeldungen unverzüglich an die Druckerei Joh. Burlage zu richten. Der Preis eines Abonnement beträgt einschließlich Mehrwertsteuer 13,00 € jährlich gegen Rechnung. Herausgegeben und verlegt vom Bischöflichen Generalvikariat Münster. Druck: Druckerei Joh. Burlage, Münster