

Der Bischof von Würzburg

Neubekanntmachung der Ordnung über den kirchlichen Datenschutz (KDO)

Die 151. Vollversammlung des Verbandes der Diözesen Deutschlands (VDD) hat in ihrer Sitzung am 18. November 2013 Änderungen der §§ 2a, 3 Abs. 5 und Abs. 6, 3a Abs. 3, 8 Abs. 2 sowie der §§ 15 ff. der „Ordnung über den kirchlichen Datenschutz (KDO)“ in der Fassung vom 1. November 2003 beschlossen und den (Erz-)Diözesen eine entsprechende Umsetzung in diözesanes Recht durch Neubekanntmachung der KDO in den jeweiligen Amtsblättern empfohlen.

Ordnung über den kirchlichen Datenschutz (KDO)

Präambel

Aufgabe der Datenverarbeitung im kirchlichen Bereich ist es, die Tätigkeit der Dienststellen und Einrichtungen der Katholischen Kirche zu fördern. Dabei muss gewährleistet sein, dass der Einzelne durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht geschützt wird. Aufgrund des Rechtes der Katholischen Kirche, ihre Angelegenheiten selbst zu regeln, wird zu diesem Zweck die folgende Ordnung erlassen:

§ 1 Zweck und Anwendungsbereich

- (1) Zweck dieser Ordnung ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.
- (2) Diese Ordnung gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch:
 1. das Bistum, die Kirchengemeinden, die Kirchenstiftungen und die Kirchengemeindeverbände,
 2. den Deutschen Caritasverband, die Diözesan-Caritasverbände, ihre Untergliederungen und ihre Fachverbände ohne Rücksicht auf ihre Rechtsform,

3. die kirchlichen Körperschaften, Stiftungen, Anstalten, Werke, Einrichtungen und die sonstigen kirchlichen Rechtsträger ohne Rücksicht auf ihre Rechtsform.
- (3) Soweit besondere kirchliche oder staatliche Rechtsvorschriften auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieser Ordnung vor. Die Verpflichtung zur Wahrung des Beicht- und Seelsorgegeheimnisses, anderer gesetzlicher Geheimhaltungspflichten oder von anderen Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

§ 2 Begriffsbestimmungen

- (1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).
- (2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.
- (3) Erheben ist das Beschaffen von Daten über den Betroffenen.
- (4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren,
 1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,
 2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
 3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
 - a) die Daten an den Dritten weitergegeben werden oder
 - b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abrufen,

4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
 5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.
- (5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.
 - (6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbarer natürlichen Person zugeordnet werden können.
 - (7) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.
 - (8) Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.
 - (9) Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Geltungsbereich dieser Ordnung personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.
 - (10) Besondere Arten personenbezogener Daten sind Angaben über die rassistische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Dazu gehört nicht die Zugehörigkeit zu einer Kirche oder sonstigen Religionsgemeinschaft.
 - (11) Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,
 1. die an den Betroffenen ausgegeben werden,
 2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und
 3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

(12) Beschäftigte sind insbesondere

1. Kleriker, Kandidaten für das Priesteramt oder in einem kirchlichen Beamtenverhältnis stehende Personen,
2. Ordensangehörige, soweit sie auf einer Planstelle in einer Einrichtung der eigenen Ordensgemeinschaft oder aufgrund eines Gestellungsvertrages tätig sind,
3. in einem Arbeitsverhältnis stehende Personen,
4. zu ihrer Berufsbildung tätige Personen mit Ausnahme der Postulanten und Novizen,
5. Teilnehmende an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobungen (Rehabilitationen),
6. in anerkannten Werkstätten für behinderte Menschen tätige Personen,
7. nach dem Bundesfreiwilligendienstgesetz oder in vergleichbaren Diensten tätige Personen,
8. Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
9. sich für ein Beschäftigungsverhältnis Bewerbende sowie Personen, deren Beschäftigungsverhältnis beendet ist.

§ 2a Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und der Aufwand nicht außer Verhältnis zum angestrebten Schutzzweck steht.

§ 3 Zulässigkeit der Datenerhebung, -verarbeitung oder -nutzung

- (1) Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist nur zulässig, soweit
 1. diese Ordnung oder eine andere kirchliche oder eine staatliche Rechtsvorschrift sie erlaubt oder anordnet oder
 2. der Betroffene eingewilligt hat.

- (2) Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Sie bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.
- (3) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Abs. 2 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Abs. 2 Satz 1 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszweckes ergibt, schriftlich festzuhalten.
- (4) Soweit besondere Arten personenbezogener Daten (§ 2 Abs. 10) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.
- (5) Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn
 1. besondere Arten personenbezogener Daten (§ 2 Abs. 10) verarbeitet werden oder
 2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.
- (6) Zuständig für die Vorabkontrolle ist der betriebliche Datenschutzbeauftragte; soweit kein betrieblicher Datenschutzbeauftragter bestellt ist, ist für die Vorabkontrolle der Diözesandatenschutzbeauftragte zuständig.

§ 3a Meldepflicht und Verzeichnis

- (1) Die in § 1 Abs. 2 genannten Stellen sind verpflichtet, Verfahren automatisierter Verarbeitung vor Inbetriebnahme dem Diözesandatenschutzbeauftragten zu melden.
- (2) Die Meldung hat folgende Angaben zu enthalten
 1. Name und Anschrift der verantwortlichen Stelle,
 2. Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung der Stelle berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
 3. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
 4. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
 5. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
 6. Regelfristen für die Löschung der Daten,
 7. eine geplante Datenübermittlung ins Ausland,
 8. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 6 KDO zur Gewährleistung der Sicherheit der Bearbeitung angemessen sind,
 9. zugriffsberechtigte Personen.
- (3) Die Meldepflicht entfällt, wenn für die verantwortliche Stelle ein betrieblicher Datenschutzbeauftragter nach § 20 bestellt wurde. Sie entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei in der Regel höchstens zehn Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.
- (4) Die Angaben nach Abs. 2 sind von der kirchlichen Stelle in einem Verzeichnis vorzuhalten. Sie macht die Angaben nach Abs. 2 Nr. 1 bis 7 auf Antrag jedermann in geeigneter Weise verfügbar, der ein berechtigtes Interesse nachweist.

§ 4 Datengeheimnis

Den bei der Datenverarbeitung tätigen Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis schriftlich zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 5 Unabdingbare Rechte des Betroffenen

- (1) Die Rechte des Betroffenen auf Auskunft (§ 13) und auf Berichtigung, Löschung oder Sperrung (§ 14) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.
- (2) Sind die Daten des Betroffenen automatisiert in einer Weise gespeichert, dass mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage, festzustellen, welche Stelle die Daten gespeichert hat, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. Der Betroffene ist über die Weiterleitung und jene zu unterrichten.

§ 5a Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

- (1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie
 1. zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts oder
 2. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zweckeerforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
- (2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.
- (3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

- (4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend § 13a zu benachrichtigen.
- (5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

§ 5b Mobile personenbezogene Speicher- und Verarbeitungsmedien

- (1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen
 1. über ihre Identität und Anschrift,
 2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,
 3. darüber, wie er seine Rechte nach den §§ 13 und 14 ausüben kann und über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmenunterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.
- (2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.
- (3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

§ 6 Technische und organisatorische Maßnahmen

Kirchliche Stellen im Geltungsbereich des § 1 Abs. 2, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieser Ordnung, insbesondere die in der Anlage zu dieser Ordnung genannten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 7 Einrichtung automatisierter Abrufverfahren

- (1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufes bleiben unberührt.
- (2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:
 1. Anlass und Zweck des Abrufverfahrens,
 2. Dritte, an die übermittelt wird,
 3. Art der zu übermittelnden Daten,
 4. nach § 6 erforderliche technische und organisatorische Maßnahmen.
- (3) Über die Einrichtung von Abrufverfahren ist der Diözesandatenschutzbeauftragte unter Mitteilung der Festlegungen des Abs. 2 zu unterrichten.
- (4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. Die speichernde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.
- (5) Die Absätze 1 bis 4 gelten nicht für den Abruf allgemein zugänglicher Daten. Allgemein zugänglich sind Daten, die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts nutzen kann.

§ 8 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

- (1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieser Ordnung und anderer Vorschriften über den Datenschutz verantwortlich. Die in § 5 genannten Rechte sind ihm gegenüber geltend zu machen.
- (2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 6 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

- (3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen diese Ordnung oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.
- (4) Die Absätze 1 bis 3 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 9 Datenerhebung

- (1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stellen erforderlich ist.
- (2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn
 1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
 2.
 - a) die zu erfüllende Aufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
 - b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

- (3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über
 1. die Identität der verantwortlichen Stelle,
 2. die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und
 3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. Werden sie beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so

ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

- (4) Werden personenbezogene Daten statt beim Betroffenen bei einer nichtkirchlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft ermächtigt, sonst auf die Freiwilligkeit ihrer Angaben, hinzuweisen.
- (5) Das Erheben besonderer Arten personenbezogener Daten (§ 2 Abs. 10) ist nur zulässig, soweit
 1. eine Rechtsvorschrift dies vorsieht oder dies aus Gründen eines wichtigen öffentlichen Interesses zwingend erforderlich ist,
 2. der Betroffene nach Maßgabe des § 3 Abs. 4 eingewilligt hat,
 3. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
 4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat oder es zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich ist,
 5. dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist oder dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,
 6. der Auftrag der Kirche oder die Glaubwürdigkeit ihres Dienstes dies erfordert,
 7. dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen,
 8. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann,

9. dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich ist.

§ 10 Datenspeicherung, -veränderung und -nutzung

- (1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.
- (2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn
 1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt und kirchliche Interessen nicht entgegenstehen,
 2. der Betroffene eingewilligt hat,
 3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
 4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
 5. die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei den, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt,
 6. es zur Abwehr einer Gefahr für die öffentliche Sicherheit oder erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
 7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,
 8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
 9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss

der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

10. der Auftrag der Kirche oder die Glaubwürdigkeit ihres Dienstes dies erfordert.
- (3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.
- (4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.
- (5) Das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten (§ 2 Abs. 10) für andere Zwecke ist nur zulässig, wenn
 1. die Voraussetzungen vorliegen, die eine Erhebung nach § 9 Abs. 5 Nr. 1 bis 6 oder 9 zulassen würden oder
 2. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das kirchliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Bei der Abwägung nach Satz 1 Nr. 2 ist im Rahmen des kirchlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.

- (6) Die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten (§ 2 Abs. 10) zu den in § 9 Abs. 5 Nr. 7 genannten Zwecken richtet sich nach den für die in § 9 Abs. 5 Nr. 7 genannten Personen geltenden Geheimhaltungspflichten.

§10a Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

- (1) Personenbezogene Daten eines Beschäftigten einschließlich der Daten über die Religionszugehörigkeit, die religiöse Überzeugung und die Erfüllung von Loyalitätsobliegenheiten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind oder eine Rechtsvorschrift dies vorsieht.
- (2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.
- (3) Die Beteiligungsrechte nach der jeweils geltenden Mitarbeitervertretungsordnung bleiben unberührt.

§ 11 Datenübermittlung an kirchliche und öffentliche Stellen

- (1) Die Übermittlung personenbezogener Daten an Stellen im Geltungsbereich des § 1 ist zulässig, wenn
 1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder der empfangenden kirchlichen Stelle liegenden Aufgaben erforderlich ist und
 2. die Voraussetzungen vorliegen, die eine Nutzung nach § 10 zulassen würden.
- (2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen der empfangenden kirchlichen Stelle, trägt diese die Verantwortung. In diesem

Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben der empfangenden kirchlichen Stelle liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. § 7 Abs. 4 bleibt unberührt.

- (3) Die empfangende kirchliche Stelle darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihr übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 10 Abs. 2 zulässig.
- (4) Für die Übermittlung personenbezogener Daten an öffentliche Stellen und an kirchliche Stellen außerhalb des Geltungsbereichs des § 1 gelten die Abs. 1–3 entsprechend, sofern sichergestellt ist, dass bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden.
- (5) Sind mit personenbezogenen Daten, die nach Abs. 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unververtretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechnete Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.
- (6) Abs. 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer kirchlichen Stelle weitergegeben werden.

§ 12 Datenübermittlung an nicht kirchliche und nicht öffentliche Stellen

- (1) Die Übermittlung personenbezogener Daten an nicht kirchliche Stellen, nicht öffentliche Stellen oder Personen ist zulässig, wenn
 1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 10 zulassen würden, oder
 2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Das Übermitteln von besonderen Arten personenbezogener Daten (§ 2 Abs. 10) ist abweichend von Satz 1 Nr. 2 nur zulässig, wenn die Voraussetzungen vorliegen, die eine Nutzung nach § 10 Abs. 5 und 6 zulassen würden oder soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.

- (2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.
- (3) In den Fällen der Übermittlung nach Abs. 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, wenn die Unterrichtung wegen der Art der personenbezogenen Daten unter Berücksichtigung der schutzwürdigen Interessen des Betroffenen nicht geboten erscheint, wenn die Unterrichtung die öffentliche Sicherheit gefährden oder dem kirchlichen Wohl Nachteile bereiten würde.
- (4) Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat ihn darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

§ 13 Auskunft an den Betroffenen

- (1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über:
 1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
 2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und
 3. den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Das Bistum bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung.

- (2) Abs.1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsgemäßer oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

- (3) Die Auskunftserteilung unterbleibt soweit,
1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,
 2. die Auskunft dem kirchlichen Wohl Nachteile bereiten würde,
 3. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden würde,
 4. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen
- und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.
- (4) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen oder rechtlichen Gründe auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an den Diözesandatenschutzbeauftragten wenden kann.
- (5) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Diözesandatenschutzbeauftragten zu erteilen, soweit nicht das Bistum im Einzelfall feststellt, dass dadurch das kirchliche Wohl beeinträchtigt wird. Die Mitteilung des Diözesandatenschutzbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.
- (6) Die Auskunft ist unentgeltlich.

§13a Benachrichtigung

- (1) Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Der Betroffene ist auch über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muss. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.

- (2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn
 1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,
 2. die Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder
 3. die Speicherung oder Übermittlung der personenbezogenen Daten durch eine Rechtsvorschrift ausdrücklich vorgesehen ist.
- (3) § 13 Abs. 2 und 3 gelten entsprechend.

§ 14 Berichtigung, Löschung oder Sperrung von Daten; Widerspruchsrecht

- (1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, dass personenbezogene Daten, die weder automatisiert verarbeitet noch in nicht automatisierten Dateien gespeichert sind, unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in geeigneter Weise festzuhalten.
- (2) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind zu löschen, wenn
 1. ihre Speicherung unzulässig ist oder
 2. ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.
- (3) An die Stelle einer Löschung tritt eine Sperrung, soweit
 1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
 2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden oder
 3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.
- (4) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.
- (5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser

Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

- (6) Personenbezogene Daten, die weder automatisiert verarbeitet noch in einer nicht automatisierten Datei gespeichert sind, sind zu sperren, wenn die verantwortliche Stelle im Einzelfall feststellt, dass ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.
- (7) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn
 1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen, im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und
 2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.
- (8) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

§ 15 Anrufung des Diözesandatenschutzbeauftragten

- (1) Wer der Ansicht ist, dass bei der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Stellen gemäß § 1 Abs. 2 gegen Vorschriften dieser Anordnung oder gegen andere Datenschutzvorschriften verstoßen worden ist oder ein solcher Verstoß bevorsteht, kann sich unmittelbar an den Diözesandatenschutzbeauftragten wenden.
- (2) Auf ein solches Vorbringen hin prüft der Diözesandatenschutzbeauftragte den Sachverhalt. Er fordert die betroffene kirchliche Dienststelle zur Stellungnahme auf, soweit der Inhalt des Vorbringens den Tatbestand einer Datenschutzverletzung erfüllt.
- (3) Niemand darf gemäßregelt oder benachteiligt werden, weil er sich im Sinne des Abs. 1 an den Diözesandatenschutzbeauftragten gewendet hat.

§ 16 Bestellung des Diözesandatenschutzbeauftragten

- (1) Der Bischof bestellt für den Bereich seines Bistums einen Diözesandatenschutzbeauftragten; die Bestellung erfolgt für die Dauer von mindestens vier, höchstens acht Jahren. Die mehrmalige erneute Bestellung ist zulässig. Die Bestellung als Datenschutzbeauftragter für mehrere Diözesen und/oder Ordensgemeinschaften ist zulässig.
- (2) Zum Diözesandatenschutzbeauftragten darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Er soll die Befähigung zum Richteramt gemäß § 5 Deutsches Richtergesetz haben und muss der Katholischen Kirche angehören. Der Diözesandatenschutzbeauftragte ist auf die gewissenhafte Erfüllung seiner Pflichten und die Einhaltung des kirchlichen und des für die Kirchen verbindlichen staatlichen Rechts zu verpflichten. Anderweitige Tätigkeiten dürfen das Vertrauen in die Unabhängigkeit und Unparteilichkeit des Diözesandatenschutzbeauftragten nicht gefährden. Dem steht eine Bestellung als Diözesandatenschutzbeauftragter für mehrere Diözesen und/oder Ordensgemeinschaften nicht entgegen.
- (3) Die Bestellung kann vor Ablauf der Amtszeit widerrufen werden, wenn Gründe nach § 24 Deutsches Richtergesetz vorliegen, die bei einem Richter auf Lebenszeit dessen Entlassung aus dem Dienst rechtfertigen, oder Gründe vorliegen, die nach der Grundordnung des kirchlichen Dienstes im Rahmen kirchlicher Arbeitsverhältnisse in der jeweils geltenden Fassung eine Kündigung rechtfertigen. Auf Antrag des Beauftragten nimmt der Bischof die Bestellung zurück.

§ 17 Rechtsstellung des Diözesandatenschutzbeauftragten

- (1) Der Diözesandatenschutzbeauftragte ist in Ausübung seiner Tätigkeit an Weisungen nicht gebunden und nur dem kirchlichen Recht und dem für die Kirchen verbindlichen staatlichen Recht unterworfen.

Die Ausübung seiner Tätigkeit geschieht in organisatorischer und sachlicher Unabhängigkeit. Die Dienstaufsicht ist so zu regeln, dass dadurch die Unabhängigkeit nicht beeinträchtigt wird.

- (2) Das der Bestellung zum Diözesandatenschutzbeauftragten zugrunde liegende Dienstverhältnis kann während der Amtszeit nur unter den Voraussetzungen des § 16 Abs. 3 beendet werden. Dieser Kündigungsschutz wirkt für den Zeitraum von einem Jahr nach der Beendigung der Amtszeit entsprechend fort, soweit ein kirchliches Beschäftigungsverhältnis fortgeführt wird oder sich anschließt.

- (3) Dem Diözesandatenschutzbeauftragten wird die für die Erfüllung seiner Aufgaben angemessene Personal- und Sachausstattung zur Verfügung gestellt. Er verfügt über einen eigenen jährlichen Haushalt, der besonders auszuweisen ist und veröffentlicht wird.
- (4) Der Diözesandatenschutzbeauftragte wählt das notwendige Personal aus, das von einer kirchlichen Stelle angestellt wird. Die vom Diözesandatenschutzbeauftragten ausgewählten und von dieser kirchlichen Stelle angestellten Mitarbeiter unterstehen der Dienst- und Fachaufsicht des Diözesandatenschutzbeauftragten und können nur mit seinem Einverständnis von der kirchlichen Stelle gekündigt, versetzt oder abgeordnet werden.
- (5) Der Diözesandatenschutzbeauftragte ist oberste Dienstbehörde im Sinne des § 96 Strafprozessordnung. Er trifft die Entscheidung über Ausgegengenehmigungen für seinen Bereich in eigener Verantwortung. Der Diözesandatenschutzbeauftragte ist oberste Aufsichtsbehörde im Sinne des § 99 Verwaltungsgerichtsordnung.
- (6) Der Diözesandatenschutzbeauftragte bestellt im Einvernehmen mit dem Diözesanbischof einen Vertreter, der im Fall seiner Verhinderung die unaufschiebbaren Entscheidungen trifft. Für den Vertreter gilt § 16 Abs. 2 entsprechend.
- (7) Der Diözesandatenschutzbeauftragte ist, auch nach Beendigung seines Auftrages, verpflichtet, über die ihm in seiner Eigenschaft als Diözesandatenschutzbeauftragtem bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.
- (8) Der Diözesandatenschutzbeauftragte darf, auch wenn sein Auftrag beendet ist, über solche Angelegenheiten ohne Genehmigung des Bischofs weder vor Gericht noch außergerichtlich Aussagen oder Erklärungen abgeben. Die Genehmigung, als Zeuge auszusagen, wird in der Regel erteilt. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen.

§ 18 Aufgaben des Diözesandatenschutzbeauftragten

- (1) Der Diözesandatenschutzbeauftragte wacht über die Einhaltung der Vorschriften dieser Ordnung sowie anderer Vorschriften über den Datenschutz. Er kann Empfehlungen zur Verbesserung des Datenschutzes geben. Des Weiteren kann er die bischöfliche Behörde und sonstige

kirchliche Dienststellen in seinem Bereich in Fragen des Datenschutzes beraten. Auf Anforderung der bischöflichen Behörde hat der Diözesandatenschutzbeauftragte Gutachten zu erstellen und Berichte zu erstatten.

- (2) Die in § 1 Abs. 2 genannten Stellen sind verpflichtet, den Diözesandatenschutzbeauftragten bei der Erfüllung seiner Aufgaben zur Unterstützung. Ihm ist dabei insbesondere
 1. Auskunft zu seinen Fragen sowie Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich in die gespeicherten Daten und in die Datenverarbeitungsprogramme,
 2. während der Dienstzeit Zutritt zu allen Diensträumen, die der Verarbeitung und Aufbewahrung automatisierter Dateien dienen, zu gewähren,soweit nicht sonstige kirchliche Vorschriften entgegenstehen.
- (3) Der Diözesandatenschutzbeauftragte erstellt jährlich einen Tätigkeitsbericht, der dem Bischof vorgelegt und der Öffentlichkeit zugänglich gemacht wird. Der Tätigkeitsbericht soll auch eine Darstellung der wesentlichen Entwicklungen des Datenschutzes im nichtkirchlichen Bereich enthalten.
- (4) Der Diözesandatenschutzbeauftragte wirkt auf die Zusammenarbeit mit den kirchlichen Stellen, insbesondere mit den anderen Diözesandatenschutzbeauftragten, hin.
- (5) Zu seinem Aufgabenbereich gehört die Zusammenarbeit mit den staatlichen Beauftragten für den Datenschutz.

§ 19 Beanstandungen durch den Diözesandatenschutzbeauftragten

- (1) Stellt der Diözesandatenschutzbeauftragte Verstöße gegen Vorschriften dieser Ordnung oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er diese unter Setzung einer angemessenen Frist zur Behebung gegenüber der betroffenen kirchlichen Dienststelle.
- (2) Wird die Beanstandung nicht fristgerecht behoben, so verständigt der Diözesandatenschutzbeauftragte die Aufsicht führende Stelle und fordert sie zu einer Stellungnahme auf.

- (3) Der Diözesandatenschutzbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der Aufsicht führenden Stelle verzichten, wenn es sich um unerhebliche Mängel handelt, deren Behebung mittlerweile erfolgt ist.
- (4) Mit der Beanstandung kann der Diözesandatenschutzbeauftragte Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.
- (5) Die gemäß Abs. 2 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandungen des Diözesandatenschutzbeauftragten getroffen worden sind.
- (6) Zur Gewährleistung der Vorschriften dieser Ordnung und anderer Vorschriften über den Datenschutz kann der Diözesandatenschutzbeauftragte gegenüber der betroffenen Dienststelle Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer und organisatorischer Mängel anordnen. Wird diese Anordnung nicht fristgemäß umgesetzt, hat sich der Diözesandatenschutzbeauftragte an die Aufsicht führende Stelle zu wenden, die zeitnah über die notwendigen Maßnahmen entscheidet.

§ 20 Betrieblicher Beauftragter für den Datenschutz

- (1) Kirchliche Stellen im Sinne des § 1 Abs. 2, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, können einen betrieblichen Datenschutzbeauftragten schriftlich bestellen.
- (2) Sind mit der automatisierten Datenerhebung, -verarbeitung oder -nutzung mehr als zehn Personen befasst, so soll ein betrieblicher Datenschutzbeauftragter bestellt werden.
- (3) Zum betrieblichen Datenschutzbeauftragten darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Mit dieser Aufgabe kann auch eine Person außerhalb der kirchlichen Stelle betraut werden. Ein betrieblicher Datenschutzbeauftragter kann von mehreren kirchlichen Stellen bestellt werden.
- (4) Der betriebliche Datenschutzbeauftragte ist dem Leiter der kirchlichen Stelle unmittelbar zu unterstellen. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden.

- (5) Die kirchlichen Stellen haben den betrieblichen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Betroffene können sich jederzeit an den betrieblichen Datenschutzbeauftragten wenden.
- (6) Ist ein betrieblicher Beauftragter für den Datenschutz bestellt worden, so ist die Kündigung seines Arbeitsverhältnisses unzulässig, es sei denn, dass Tatsachen vorliegen, welche die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung der Kündigungsfrist berechtigen. Nach der Abberufung als betrieblicher Beauftragter für den Datenschutz ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, es sei denn, dass die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.
- (7) Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde hat die verantwortliche Stelle dem betrieblichen Beauftragten für den Datenschutz die Teilnahme an Fort- und Weiterbildungsveranstaltungen in angemessenem Umfang zu ermöglichen und deren Kosten zu übernehmen.
- (8) Im Übrigen findet § 16 entsprechende Anwendung.
- (9) Sind mit der automatisierten Datenerhebung, -verarbeitung oder -nutzung weniger als elf Personen befasst, kann die Erfüllung der Aufgaben des betrieblichen Datenschutzes in anderer Weise geregelt werden.

§ 21 Aufgaben des betrieblichen Datenschutzbeauftragten

- (1) Der betriebliche Datenschutzbeauftragte wirkt auf die Einhaltung dieser Ordnung und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann er sich in Zweifelsfällen an den Diözesandatenschutzbeauftragten gem. § 16 KDO wenden. Er hat insbesondere
 1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,
 2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieser Ordnung sowie anderer Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

- (2) Dem betrieblichen Datenschutzbeauftragten ist von der verantwortlichen Stelle eine Übersicht nach § 3a Abs. 2 zur Verfügung zu stellen.
- (3) Der betriebliche Datenschutzbeauftragte macht die Angaben nach § 3a Abs. 2 Nr. 1 bis 7 auf Antrag jedermann in geeigneter Weise verfügbar, der ein berechtigtes Interesse nachweist.

§ 22 Ermächtigungen

Die zur Durchführung dieser Ordnung erforderlichen Regelungen trifft der Generalvikar. Er legt insbesondere fest:

- a) den Inhalt der Meldung gemäß § 3a,
- b) den Inhalt der schriftlichen Verpflichtungserklärung gemäß § 4 Satz 2,
- c) die technischen und organisatorischen Maßnahmen gemäß § 6 Satz 1.
- d) die Erfüllung der Aufgaben des betrieblichen Datenschutzes gemäß § 20 Abs. 9.

§ 23 Schlussbestimmung

Diese Ordnung tritt am 1. Mai 2014 in Kraft.

Gleichzeitig tritt die Ordnung über den kirchlichen Datenschutz (KDO) vom 1. November 2003 (Würzburger Diözesanblatt 149 (2003) Nr. 17 vom 25.10.2003) sowie deren Änderungen (Würzburger Diözesanblatt 156 (2010) Nr. 20 vom 15.11.2010 und Würzburger Diözesanblatt 159 (2013) Nr. 12 vom 01.07.2013) außer Kraft.

Würzburg, 25. März 2014

+ Friedhelm
Bischof von Würzburg

Für Fragen, die die kirchliche Datenschutzordnung betreffen, stehen folgende Personen zur Verfügung:

- Herr Justitiar und betrieblicher Datenschutzbeauftragter Roland Huth, Tel.: (09 31) 3 86 - 2 47, Mail: rechtsabteilung@bistum-wuerzburg.de
- Herr Jupp Joachimski, Datenschutzbeauftragter der bayerischen (Erz-) Diözesen, Mail: jjoachimski@eomuc.de

Generalvikar

Verordnung zur Durchführung der Ordnung über den kirchlichen Datenschutz (KDO-DVO)

Aufgrund des § 22 der Ordnung über den kirchlichen Datenschutz (KDO) in der Fassung der Bekanntmachung vom 25. März 2014 (Würzburger Diözesanblatt 160 (2014) Nr. 7 vom 15.04.2015) wird die Verordnung zur Durchführung der Ordnung über den kirchlichen Datenschutz (KDO-DVO) in der Fassung der Bekanntmachung vom 16. September 2003 (Würzburger Diözesanblatt 149 (2003) Nr. 17 vom 25.10.2003) wie folgt neu gefasst:

I. Zu § 3 a KDO (Meldung von Verfahren automatisierter Verarbeitung)

- (1) Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind diese vor Inbetriebnahme schriftlich dem Diözesandatenschutzbeauftragten zu melden. Sofern ein betrieblicher Datenschutzbeauftragter bestellt ist, ist diesem gemäß § 18 b Abs. 2 KDO eine Übersicht nach § 3 a Abs. 2 KDO zur Verfügung zu stellen.
- (2) Für die Meldung von Verfahren automatisierter Verarbeitung vor Inbetriebnahme beziehungsweise die dem betrieblichen Datenschutzbeauftragten zur Verfügung zu stellende Übersicht soll das Muster gemäß der Anlage verwandt werden.

II. Zu § 4 KDO

- (1) Zum Kreis der bei der Datenverarbeitung tätigen Personen im Sinne des § 4 KDO gehören die in den Stellen gemäß § 1 Abs. 2 KDO gegen Entgelt beschäftigten und ehrenamtlich tätigen Personen. Sie werden belehrt über:
 1. den Inhalt der KDO und anderer für ihre Tätigkeit geltender Datenschutzvorschriften; dies geschieht durch Hinweis auf die für den Aufgabenbereich des Mitarbeiters wesentlichen Grundsätze und im übrigen auf die Texte in der jeweils gültigen Fassung. Diese Texte werden zur Einsichtnahme und etwaigen kurzfristigen Ausleihe bereitgehalten; dies wird dem Mitarbeiter bekannt gegeben,
 2. die Verpflichtung zur Beachtung der in Nummer 1 genannten Vorschriften bei ihrer Tätigkeit in der Datenverarbeitung,

3. mögliche disziplinarrechtliche bzw. arbeitsrechtliche/rechtliche Folgen eines Verstoßes gegen die KDO und andere für ihre Tätigkeit geltende Datenschutzvorschriften,
 4. das Fortbestehen des Datengeheimnisses nach Beendigung der Tätigkeit bei der Datenverarbeitung.
- (2) Über die Beachtung der Verpflichtung ist von den bei der Datenverarbeitung tätigen Personen eine schriftliche Erklärung nach näherer Maßgabe des Abschnittes III abzugeben. Die Urschrift der Verpflichtungserklärung wird zu den Personalakten der bei der Datenverarbeitung tätigen Personen genommen, welche eine Ausfertigung der Erklärung erhalten.
- (3) Die Verpflichtung auf das Datengeheimnis erfolgt durch den Dienstvorgesetzten der in der Datenverarbeitung tätigen Personen oder einen von ihm Beauftragten.

III. Zu § 4 KDO

- (1) Die schriftliche Verpflichtungserklärung der bei der Datenverarbeitung tätigen Personen gemäß § 4 Satz 2 KDO hat zum Inhalt,
1. Angaben zur Identifizierung (Vor- und Zuname, Geburtsdatum und Anschrift sowie Beschäftigungsdienststelle),
 2. die Bestätigung,
 - a) dass auf die für den Aufgabenbereich des Mitarbeiters wesentlichen Grundsätze und im Übrigen auf die Texte in der jeweils gültigen Fassung sowie
 - b) auf die Möglichkeit der Einsichtnahme und etwaigen kurzfristigen Ausleihe dieser Texte hingewiesen wurde,
 3. die Verpflichtung, die KDO und andere für ihre Tätigkeit geltende Datenschutzvorschriften in der jeweils gültigen Fassung sorgfältig einzuhalten, die Bestätigung, dass sie über disziplinarrechtliche bzw. arbeitsrechtliche/rechtliche Folgen eines Verstoßes gegen die KDO belehrt wurden.
- (2) Die schriftliche Verpflichtungserklärung ist von der bei der Datenverarbeitung tätigen Person unter Angabe des Ortes und des Datums der Unterschriftsleistung zu unterzeichnen.
- (3) Für die schriftliche Verpflichtungserklärung sind die Muster gemäß der Anlage zu verwenden.

IV. Zu § 6 KDO

Anlage 1 zu § 6 KDO:

Werden personenbezogene Daten automatisiert, verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Anlage 2 zu § 6 KDO:

1.0 Aufgaben und Ziele dieser Anlage

Diese Anlage regelt den Einsatz von Arbeitsplatzcomputern in kirchlichen Stellen. Sie ist als Ergänzung zu § 6 der Anordnung über den Kirchlichen Datenschutz (KDO) und den zu ihr ergangenen bereichsspezifischen Datenschutzregelungen in ihren jeweils geltenden Fassungen anzusehen.

2.0 Arbeitsplatzcomputer/Datenverarbeitungsanlage

- Arbeitsplatzcomputer (APC) im Sinne dieser Anlage sind alle selbständigen Systeme der Datenverarbeitung, die von einer kirchlichen Stelle im Sinne des § 1 Abs. 2 KDO zur Erfüllung ihrer Aufgaben genutzt werden.
- Sie können als Einzelgerät (Stand-Alone-PC) oder in Verbindung mit anderen APC (Netzwerken) bzw. anderen Systemen als Datenverarbeitungsanlage installiert sein.
- Als APC sind z. B. auch tragbare Geräte (Laptops bzw. Notebooks oder Netbooks), Tabletcomputer und Mobiltelefone sowie Drucker bzw. Kopierer mit eigener Speichereinheit zu behandeln.

3.0 Allgemeine Grundsätze

3.1 Verantwortlichkeit der Mitarbeiter

- Mitarbeiter im Sinne dieser Anlage sind über die in § 2 Abs. 12 KDO genannten Beschäftigten hinaus auch ehrenamtlich für kirchliche Stellen tätige Personen, die APC verwenden.
- Jeder Mitarbeiter trägt die datenschutzrechtliche Verantwortung für eine vorschriftsmäßige Ausübung seiner Tätigkeit. Es ist ihm untersagt, personenbezogene Daten zu einem anderen als dem in der jeweils rechtmäßigen Aufgabenerfüllung liegenden Zweck zu verarbeiten oder zu übermitteln.

3.2 Verantwortlichkeit der Dienststellenleiter

- Die jeweils als Dienststellenleiter verantwortliche Person ist durch den Generalvikar oder durch die sonst vorgesetzte Dienststelle zu bestimmen.
- Der Dienststellenleiter legt fest, welche im Sinne der KDO schutzwürdigen Daten auf Datenverarbeitungsanlagen gespeichert und verarbeitet werden.

- Ihm obliegt die zutreffende Einordnung der jeweiligen Daten in die Datenschutzklassen nach dieser Anlage zur KDO-DVO.
- Der Dienststellenleiter klärt die Mitarbeiter über die Gefahren, die aus der Nutzung einer Datenverarbeitungsanlage erwachsen, sowie über den möglichen Schaden, der kirchlichen Einrichtungen aus einer Datenschutzverletzung erwachsen kann, auf.
- Der Dienststellenleiter stellt sicher, dass ein Konzept zur datenschutzrechtlichen Ausgestaltung der Datenverarbeitungsanlagen erstellt wird.
- Der Dienststellenleiter kann seine Aufgaben und Befugnisse nach dieser Durchführungsverordnung durch schriftliche Anordnung auf geeignete Mitarbeiter übertragen.

3.3 Technische und organisatorische Maßnahmen

Mit der Eingabe, Speicherung, Verarbeitung und Nutzung personenbezogener Daten auf Anlagen der elektronischen Datenverarbeitung darf erst begonnen werden, wenn die datenverarbeitende Stelle die nach der Anlage 1 zu § 6 KDO und die nach dieser Anlage erforderlichen technischen und organisatorischen Maßnahmen zum Schutz dieser Daten getroffen hat.

3.4 Mindestanforderungen

Unabhängig vom Grad der Schutzbedürftigkeit der Daten sind dabei zumindest folgende Maßnahmen zu treffen:

- Das nach § 3 a Abs. 4 KDO zu führende Verzeichnis hat darüber hinaus den regelmäßigen Nutzer, den Standort und die interne Kennzeichnungs-Nummer zu enthalten.
- Alle bei der Verarbeitung personenbezogener Daten beteiligten Personen haben die Verpflichtungserklärung gemäß § 4 Abs. 2 Satz 1 KDO abzugeben. Den Mitarbeitern, die die Verpflichtungserklärung unterschrieben haben, sind die jeweils gültige Anordnung über den Kirchlichen Datenschutz, etwaige Verordnungen, Dienstanordnungen oder Dienstvereinbarungen und die in ihrem Arbeitsbereich zu beachtenden bereichsspezifischen Datenschutzregelungen (Schulen, Krankenhäuser, Friedhöfe etc.) in geschäftsüblicher Weise zugänglich zu machen.
- Es ist sicherzustellen, dass auf dienstlich genutzten Anlagen der elektronischen Datenverarbeitung ausschließlich autorisierte Programme zu dienstlichen Zwecken verwendet werden. Die Benutzung privater Programme ist unzulässig.

- Werden Daten aus den Melderegistern der kommunalen Meldebehörden in kirchlichen Rechenzentren verarbeitet, so orientieren sich die Schutzmaßnahmen an den BSI-IT-Grundschutzkatalogen. Rechenzentren im Sinne dieser Vorschrift sind die für den Betrieb von größeren, zentral in mehreren Dienststellen eingesetzten Informations- und Kommunikationssystemen erforderlichen Einrichtungen.

4.0 Datenschutzklassen

- Das Ausmaß der möglichen Gefährdung personenbezogener Daten bestimmt Art und Umfang der Sicherungsmaßnahmen. Zur Erleichterung der Einordnung bedient sich diese Anlage der Definition dreier Datenschutzklassen, die sich aus der Art der zu verarbeitenden Daten ergeben. Dem Dienststellenleiter, der die Einordnung vornimmt, steht es frei, aus Gründen des Einzelfalles die zu verarbeitenden Daten anders einzuordnen als hier vorgesehen. Diese Gründe sollen kurz dokumentiert werden.
- Bei der Einordnung in die einzelnen Datenschutzklassen ist auf die Daten abzustellen, die vom Benutzer bewusst bearbeitet und gespeichert werden.

4.1 Datenschutzklasse I

Zur Datenschutzklasse I gehören personenbezogene Daten, deren Missbrauch keine besonders schwer wiegende Beeinträchtigung des Betroffenen erwarten lässt. Hierzu gehören insbesondere Adressangaben ohne Sperrvermerke, z. B. Berufs-, Branchen- oder Geschäftsbezeichnungen.

4.2 Datenschutzklasse II

Zur Datenschutzklasse II gehören personenbezogene Daten, deren Missbrauch 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, usw.

4.3 Datenschutzklasse III

Zur Datenschutzklasse III gehören personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann. Hierzu gehören z. B. Daten über kirchliche Amtshandlungen, gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen, die Mitgliedschaft in einer Religionsgesellschaft, arbeitsrechtliche Rechtsverhältnisse, Disziplinaentscheidungen, usw. sowie Adressangaben mit Sperrvermerken.

4.4 Nicht elektronisch zu verarbeitende Daten

Daten, deren Kenntnis dem Beicht- oder Seelsorgegeheimnis unterliegen sowie Daten über die Annahme einer Person an Kindes statt (Adoptionsgeheimnis) sind in besonders hohem Maße schutzbedürftig. Ihre Ausspähung oder Verlautbarung würde dem Vertrauen in die Verschwiegenheit katholischer Dienststellen und Einrichtungen schweren Schaden zufügen. Daher dürfen diese Daten nicht auf APC verarbeitet werden, es sei denn, es handelte sich um aus dem staatlichen Bereich übernommene Daten.

4.5 Einordnung in die Datenschutzklassen

- Bei der Einordnung der zu speichernden personenbezogenen Daten in die vorgenannten Schutzklassen ist auch deren Zusammenhang mit anderen gespeicherten Daten, der Zweck ihrer Verarbeitung und das anzunehmende Missbrauchsinteresse zu berücksichtigen.
- Die Einordnung spricht der Dienststellenleiter aus; er soll einen etwa bestellten betrieblichen Datenschutzbeauftragten und kann den Diözesan-datenschutzbeauftragten dazu anhören.
- Wenn keine Einordnung festgelegt ist, gilt automatisch die Datenschutzklasse III, sofern nicht die Voraussetzungen der Ziffer 4.4 vorliegen.

5.0 Besondere Gefahrenlagen

5.1 Nutzung privater Datenverarbeitungssysteme zu dienstlichen Zwecken

Die Verarbeitung personenbezogener Daten auf privaten Datenverarbeitungssystemen zu dienstlichen Zwecken ist grundsätzlich unzulässig. Unter bestimmten Voraussetzungen kann sie als Ausnahme vom Dienststellenleiter genehmigt werden. Die Genehmigung erfolgt schriftlich unter Nennung der Gründe.

5.2 Fremdzugriffe

Der Zugriff aus und von anderen Datenverarbeitungsanlagen durch Externe (z. B. Fremdfirmen, fremde Dienststellen) schafft besondere Gefahren hinsichtlich der Ausspähung von Daten. Minimalanforderung ist eine Verpflichtung des Externen auf die KDO. Art und Umfang der Zugriffe sind auf ein Mindestmaß zu reduzieren und gesondert zu regeln.

Für die Fernwartung gilt § 8 KDO entsprechend.

V. Zu § 12 Abs. 3 KDO

- (1) Die Unterrichtung des Betroffenen (§ 2 Abs. 1 KDO) über eine Übermittlung gemäß § 12 Abs. 3 Satz 1 KDO erfolgt schriftlich.
- (2) Sie enthält
 1. die Bezeichnung der übermittelnden Stelle einschließlich der Anschrift,
 2. die Bezeichnung des Dritten, an den die Daten übermittelt werden, einschließlich der Anschrift,
 3. die Bezeichnung der übermittelten Daten.

VI. Zu § 13 Abs. 1 KDO

- (1) Der Antrag des Betroffenen (§ 2 Abs. 1 KDO) auf Auskunft ist schriftlich an die verantwortliche Stelle (§ 2 Abs. 8 KDO) zu richten oder dort zu Protokoll zu erklären.
- (2) Der Antrag soll die Art der personenbezogenen Daten, über die Auskunft begehrt wird, näher bezeichnen. Der Antrag auf Auskunft über personenbezogene Daten, die weder automatisiert verarbeitet noch in einer nicht automatisierten Datei gespeichert sind, muss Angaben enthalten, die das Auffinden der Daten ermöglichen.
- (3) Der Antrag kann beschränkt werden auf Auskunft über
 1. die zur Person des Betroffenen gespeicherten Daten oder
 2. die Herkunft dieser Daten oder
 3. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben worden sind oder
 4. den Zweck, zu dem diese Daten gespeichert sind.
- (4) Vorbehaltlich der Regelung in § 13 Abs. 3 KDO wird die Auskunft in dem beantragten Umfang von der verantwortlichen Stelle (§ 2 Abs. 8 KDO) schriftlich erteilt.
- (5) Wenn die Erteilung der beantragten Auskunft gemäß § 13 Abs. 2 oder 3 KDO zu unterbleiben hat, so ist dies dem Antragsteller schriftlich mitzuteilen. Die Versagung der beantragten Auskunft soll begründet werden. Für den Fall, dass eine Begründung gemäß § 13 Abs. 4 KDO nicht erforderlich ist, ist der Antragsteller darauf hinzuweisen, dass er sich an den Diözesandatenschutzbeauftragten wenden kann; die Anschrift des Diözesandatenschutzbeauftragten ist ihm mitzuteilen.

VII. Zu § 13 a KDO

- (1) Die Benachrichtigung des Betroffenen (§ 2 Abs. 1 KDO) gemäß § 13 a Abs. 1 KDO erfolgt, soweit die Pflicht zur Benachrichtigung nicht nach § 13 a Abs. 2 und 3 entfällt, schriftlich durch die verantwortliche Stelle.
- (2) Sie enthält
 1. die zur Person des Betroffenen gespeicherten Daten,
 2. die Bezeichnung der verantwortlichen Stelle,
 3. den Zweck, zu dem die Daten erhoben, verarbeitet oder genutzt werden.
 4. die Empfänger oder Kategorien von Empfängern, soweit der Betroffene nicht mit der Übermittlung an diese rechnen muss.

VIII. Zu § 14 KDO

- (1) Der Betroffene (§ 2 Abs. 1 KDO) kann schriftlich beantragen, ihn betreffende personenbezogene Daten zu berichtigen oder zu löschen. Der Antrag ist schriftlich an die Stellen gemäß § 1 Abs. 2 Nr. 2 und 3, im Falle des § 1 Abs. 2 Nr. 1 an das Bistum zu richten.
- (2) In dem Antrag auf Berichtigung sind die Daten zu bezeichnen, deren Unrichtigkeit behauptet wird. Der Antrag muss Angaben über die Umstände enthalten, aus denen sich die Unrichtigkeit der Daten ergibt.
- (3) In dem Antrag auf Löschung sind die personenbezogenen Daten zu bezeichnen, deren Speicherung für unzulässig gehalten wird. Der Antrag muss Angaben über die Umstände enthalten, aus denen sich die Unzulässigkeit der Speicherung ergibt.
- (4) Die zuständige Stelle entscheidet schriftlich über Anträge gemäß Abs. 1. Die Entscheidung ist dem Antragsteller bekannt zu geben. Im Falle des § 14 Abs. 8 KDO sind ihm die Stellen anzugeben, die von der Berichtigung, Löschung oder Sperrung verständigt worden sind. Ist eine Verständigung aufgrund des § 14 Abs. 8 KDO unterblieben, sind dem Antragsteller die Gründe dafür mitzuteilen.
- (5) Der Widerspruch gemäß § 14 Abs. 5 KDO ist schriftlich oder zur Niederschrift bei der verantwortlichen Stelle (§ 2 Abs. 8 KDO) einzulegen. Die Umstände, aus denen sich das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation ergibt, sind von dem Betroffenen darzulegen. Die verantwortliche Stelle entscheidet über den Widerspruch in geeigneter Form. Die Entscheidung ist dem Betroffenen bekannt zu geben.

IX. Inkrafttreten

- (1) Diese Fassung der Verordnung zur Durchführung der Ordnung über den kirchlichen Datenschutz (KDO – DVO) tritt am 1. November 2015 in Kraft.
- (2) Gleichzeitig tritt die Verordnung zur Durchführung der Ordnung über den kirchlichen Datenschutz (KDO-DVO) in der Fassung der Bekanntmachung vom 16. September 2003 (Würzburger Diözesanblatt 149 (2003) Nr. 17 vom 25.10.2003) außer Kraft.

Würzburg, 12. Oktober 2015

Thomas Keßler
Generalvikar

Anlagen

1. Zu Abschnitt I. KDO-DVO (§ 3 a KDO Meldung von Verfahren automatisierter Verarbeitungen)

Die Notwendigkeit für die in den nachfolgenden Formularen (Muster 1 und Muster 2) geforderten Angaben ergibt sich aus § 3 a KDO. Für jedes automatisierte Verfahren einer verantwortlichen Stelle füllt der Rechtsträger (§ 1 Abs. 2 KDO) ein Formular nach Muster 1 und Muster 2 aus.

Allgemeine Angaben (§ 3 a Abs. 2 Nr. 1 und Nr. 2 KDO)**1. Name und Anschrift**

- 1.1 des Rechtsträgers (§ 1 Abs. 2 KDO) (z. B. *Kirchenstiftung*)
- 1.2 der verantwortlichen Stelle (Jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt [§ 2 Abs. 8 KDO]) (z. B. *Kindergarten der Kirchenstiftung*)

2. Vertretung der verantwortlichen Stelle

- 2.1 der nach der Verfassung (Statut, Geschäftsordnung, Satzung) berufene Leiter der verantwortlichen Stelle (z. B. *Leiterin des Kindergartens der Kirchenstiftung*)
- 2.2 mit der Leitung der Datenverarbeitung in der verantwortlichen Stelle beauftragte Personen (z. B. *beauftragte Gruppenleiterin im Kindergarten der Kirchenstiftung*)

Besondere Angaben (§ 3 a Abs. 2 Nr. 3 bis Nr. 7 KDO)

3. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung (z. B. *Mitglieder- und Bestandspflege*)
4. Betroffene Personengruppen und Daten oder Datenkategorien
 - 4.1 Beschreibung der betroffenen Personengruppen (z. B. *Arbeitnehmer, Gemeindemitglieder, Patienten usw.*)
 - 4.2 Beschreibung der diesbezüglichen Daten oder Datenkategorien (*Mit „Daten“ sind „personenbezogene Daten“ i. S. d. § 2 Abs. 1 KDO gemeint, wie z. B. Name, Anschrift, Geburtsdatum, Religionszugehörigkeit. Grundsätzlich reicht jedoch die Angabe von Datenkategorien, z. B. Personaldaten, aus. Sogenannte „besondere Arten personenbezogener Daten“ (vgl. § 2 Abs. 10 KDO) sind entsprechend anzugeben.*)
5. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können (Jede Person oder Stelle, die Daten erhält [§ 2 Abs. 9 KDO]) (z. B. *Behörden, kirchliche Stellen, Versicherungen, ärztliches Personal usw.*)
6. Regelfristen für die Löschung der Daten
7. Geplante Datenübermittlung ins Ausland

 Ort, Datum

 Unterschrift

Allgemeine Angaben (§ 3 a Abs. 2 Nr. 1 und Nr. 2 KDO)

1. Name und Anschrift

- 1.1 des Rechtsträgers (§ 1 Abs. 2 KDO) (z. B. *Kirchenstiftung*)
- 1.2 der verantwortlichen Stelle (*Jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt [§ 2 Abs. 8 KDO]*) (z. B. *Kindergarten der Kirchenstiftung*)

2. Vertretung der verantwortlichen Stelle

- 2.1 der nach der Verfassung (Statut, Geschäftsordnung, Satzung) berufene Leiter der verantwortlichen Stelle (z. B. *Leiterin des Kindergartens der Kirchenstiftung*)
- 2.2 mit der Leitung der Datenverarbeitung in der verantwortlichen Stelle beauftragte Personen (z. B. *beauftragte Gruppenleiterin im Kindergarten der Kirchenstiftung*)

Besondere Angaben (§ 3 a Abs. 2 Nr. 8 und Nr. 9 KDO)

- 3. Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (z. B. Konfigurationsübersicht, Netzwerkstruktur, Betriebs- und Anwendungssoftware, spezielle Sicherungssoftware usw.)
- 4. Zugriffsberechtigte Personen

Ort, Datum

Unterschrift

2. Zu Abschnitt III. KDO-DVO (§ 4 Satz 2 KDO):

Muster für Verpflichtungserklärungen für Hauptberufliche, Ehrenamtliche und Externe:

Verpflichtungserklärung für Hauptberufliche gem. § 4 S. 2 KDO

Belehrung und Verpflichtung auf das Datengeheimnis

nach § 4 der Ordnung über den kirchlichen Datenschutz (KDO)

Herr/Frau _____, geb. am _____
(Vor- und Zuname)

wohnhaft _____

Dienststelle _____

- I. Über Aufgabe und Gegenstand des Datenschutzes im kirchlichen Bereich werden Sie nachfolgend gemäß § 4 KDO belehrt, da Sie in Ihrem Tätigkeitsbereich mit personenbezogenen bzw. dienstlichen Daten befasst sind:
 1. Aufgabe des Datenschutzes im kirchlichen Bereich ist es, durch den Schutz personenbezogener Daten vor Missbrauch bei ihrer Speicherung, Übermittlung, Veränderung und Löschung, der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken.
 2. Bei der Verarbeitung und Speicherung von Daten, insbesondere personenbezogenen Daten, sind die Datenschutzvorschriften gemäß der Ordnung über den kirchlichen Datenschutz (KDO) und der hierzu ergangenen Durchführungsverordnung (KDO-DVO) zu beachten.
 3. Es ist insbesondere untersagt, geschützte personenbezogene Daten zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekannt zu geben, zugänglich zu machen oder sonst zu nutzen.

4. Zugeteilte Benutzernamen und Passwörter sind vertraulich zu behandeln und dürfen nicht an Unberechtigte weitergegeben werden. Bei Verlassen des Arbeitsplatzes (Pausen, Zeiten sonstiger Abwesenheit) sind die Systeme vor unberechtigtem Zugriff bzw. unberechtigter Einsichtnahme zu schützen. Für Notfälle sind beim Dienststellenleiter die aktuellen Passwörter verschlossen zu hinterlegen.
5. Die private Nutzung der Arbeitsplatzcomputer (APC) ist grundsätzlich nicht erlaubt. Insbesondere ist es untersagt, fest installierte APC vom Arbeitsplatz zu entfernen, Software für den privaten Gebrauch (z. B. Spiele, Demos, Zeitschriften-CDs, Hilfsprogramme, Einkommensteuerprogramme, Bildschirmschoner, Hintergrundbilder, u. ä.) auf dem APC zu installieren und zu betreiben; Dateien, Datenbanken, etc. im Arbeitsspeicher oder auf der Festplatte zum privaten Gebrauch einzurichten, es sei denn, es ist vom Systembetreuer hierfür ein spezieller Bereich ausgewiesen (privates Unterverzeichnis); Programme, Daten, Internet, E-Mail, usw. für sonstige dienstfremde Zwecke zu verwenden oder betriebsfremden Personen oder Institutionen zur Verfügung zu stellen oder in sonstiger Weise zugänglich zu machen.
6. Grundsätzlich dürfen die Internetdienste am Arbeitsplatz nur dienstlich genutzt werden. Der Dienststellenleiter kann bis auf Widerruf die Nutzung des Internetzugangs außerhalb der Arbeitszeit auch zu privaten Zwecken in begrenztem geringen Umfang dulden, wenn dadurch der Betriebsablauf nicht gestört wird und dem Dienstgeber keine zusätzlichen Kosten hierdurch entstehen. Der/die Mitarbeiter/in, der/die privat das Internet trotz der grundsätzlichen Untersagung nutzt, erklärt sich mit der Nutzung einverstanden, dass die Protokolldateien wie für den dienstlichen Gebrauch ausgewertet werden und unterwirft sich den Seitenzugangsbeschränkungen durch die Diözese.
7. Unzulässig ist dabei jede Nutzung von E-mail bzw. Internet, die objektiv geeignet ist, den Interessen der Katholischen Kirche oder deren Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Gesetze und/oder Verordnungen verstößt, z. B. Abrufen oder Anbieten/Versenden von Inhalten, die offensichtlich gegen Datenschutz-, Persönlichkeits-, Urheber- oder strafrechtliche Bestimmungen verstoßen und/oder von beleidigenden, verleumderischen, verfassungsfeindlichen, gewaltverherrlichenden, rassistischen, sexistischen oder pornografischen Äußerungen oder Abbildungen.

8. Den EDV-Administratoren oder den dafür Beauftragten ist die Einsicht und die Nutzung von Protokolldaten, also z. B. Gebührenausswertungen bei Telefonen, das Internetprotokoll, für Zwecke der Systemsicherheit, Systemintegrität und einer Kontrolle nach der Regelung zur Nutzungsbeschränkung von Internetdiensten gestattet. Der Dienstgeber ist berechtigt, bis zu viermal im Jahr Stichproben der Protokolle über die Nutzung der Internetdienste aus dem laufenden oder dem Vormonat zu veranlassen.
 9. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit im kirchlichen Dienst fort.
 10. Verstöße gegen das Datengeheimnis sind gleichzeitig Verstöße gegen die Schweigepflicht und können rechtlich, insbesondere arbeitsrechtliche Folgen nach sich ziehen.
 11. Besonders hingewiesen wird auf die „Regelung zur Kontrolle der Nutzungsbeschränkung von Internetdiensten (ABD, Teil C, 10 b)“ und auf die „Dienstvereinbarung über die Nutzung neuer Informations- und Kommunikationstechnologien“. Diese Regelungswerke können, wie die KDO selbst, beim Personalleiter, der Mitarbeitervertretung (MAV), bzw. im Internet unter www.bistum-wuerzburg.de im geschützten Bereich eingesehen werden.
- II. Der/die Mitarbeiter/in bestätigt durch seine/ihre Unterschrift über Aufgabe und Gegenstand des Datenschutzes im kirchlichen Bereich belehrt worden zu sein. Ferner verpflichtet er/sie sich, die Ordnung über den kirchlichen Datenschutz (KDO) und die damit zusammenhängenden Regelungswerke sorgfältig einzuhalten.

Diese Erklärung wird zu den Personalakten genommen.

Ort, Datum _____

Unterschrift _____
(Vor- und Zuname)

Verpflichtungserklärung für Ehrenamtliche gem. § 4 KDO

Verpflichtung auf das Datengeheimnis

Verpflichtungserklärung für Ehrenamtliche
nach § 4 der Ordnung über den kirchlichen Datenschutz (KDO)

Ich, _____, geb. am _____
(Vor- und Zuname)

wohnhaft _____

bin bei _____

ehrenamtlich tätig.

Ich verpflichte mich,

1. die Ordnung über den kirchlichen Datenschutz (KDO) des Bistums Würzburg sowie die anderen für meine ehrenamtliche Tätigkeit geltenden Datenschutzregelungen einschließlich der zu ihrer Durchführung ergangenen Bestimmungen in ihrer jeweils geltenden Fassung sorgfältig einzuhalten und alle personenbezogenen Angaben, die ich aufgrund meines Ehrenamtes erhalte oder die mir im Zusammenhang mit meinem Ehrenamt zur Kenntnis gelangen, während meiner ehrenamtlichen Tätigkeit vertraulich zu behandeln.

Ich wurde ferner darauf hingewiesen, dass die KDO und die Texte der übrigen für meine ehrenamtliche Tätigkeit geltenden Datenschutzvorschriften im _____ bzw. bei _____ eingesehen und auch für kurze Zeit ausgeliehen werden können.

2. das Datengeheimnis auch nach Beendigung meiner ehrenamtlichen Tätigkeit zu beachten.

Ich bin darüber belehrt worden, dass ein Verstoß gegen das Datengeheimnis zum Entzug des Ehrenamtes führen kann. Auf mögliche Schadensersatzansprüche, die aus einer unzulässigen Weitergabe personenbezogener Daten resultieren können, wurde ich hingewiesen.

Diese Erklärung wird zu den Akten genommen.

Ort, Datum _____

Unterschrift _____
(Vor- und Zuname)

Verpflichtungserklärung für Externe gem. § 4 KDO

Verpflichtung auf das Datengeheimnis

Verpflichtungserklärung für Externe
nach § 4 der Ordnung über den kirchlichen Datenschutz (KDO)

Ich, _____, geb. am _____
(Vor- und Zuname)

wohnhaft _____

werde im Rahmen meiner Tätigkeit für die _____^{1.}

bei _____ tätig.

Ich verpflichte mich,

1. die Ordnung über den kirchlichen Datenschutz (KDO) des Bistums Würzburgs sowie die anderen für meine Tätigkeit geltenden Datenschutzregelungen einschließlich der zu ihrer Durchführung ergangenen Bestimmungen in ihrer jeweils geltenden Fassung sorgfältig einzuhalten und alle personenbezogenen Angaben, die ich aufgrund meiner Tätigkeit erhalte oder die mir im Zusammenhang hiermit zur Kenntnis gelangen, während meiner Tätigkeit vertraulich zu behandeln. Ich bestätige, dass ich auf die wesentlichen Grundsätze der für meine Tätigkeit geltenden Bestimmungen hingewiesen wurde. Ich wurde ferner darauf hingewiesen, dass die KDO und die Texte der übrigen für meine Tätigkeit geltenden Datenschutzvorschriften bei _____^{2.} eingesehen und auch für kurze Zeit ausgeliehen werden können.
2. das Datengeheimnis auch nach Beendigung meiner Tätigkeit zu beachten.

Ich bin darüber belehrt worden, dass ein Verstoß gegen das Datengeheimnis gleichzeitig einen Verstoß gegen die Schweigepflicht darstellt, der rechtliche Folgen haben kann.

Diese Erklärung wird zu den Akten genommen.

Ort, Datum _____

Unterschrift _____
(Vor- und Zuname)

- _____
- ^{1.} Firma einsetzen, bei der der externe Dienstleister angestellt ist.
 - ^{2.} Bereich einsetzen, in dem der externe Dienstleister tätig wird.

IT-Richtlinien
zur Umsetzung von IV. Anlage 2 zu § 6 KDO
der Durchführungsverordnung zur
Ordnung über den kirchlichen Datenschutz (KDO-DVO)

Präambel

Die IT-Richtlinien definieren einen Mindeststandard für den kirchlichen Datenschutz. Dieser dient auch dazu, die überdiözesane Zusammenarbeit zu erleichtern (Datenschutzkonformität).

Die zu etablierenden Datenschutzklassen (DSK) sind sowohl auf personenbezogene als auch auf schützenswerte nicht personenbezogene Daten anzuwenden (z. B. auf Buchhaltungsdaten (= DSK II) und Kirchensteuerdaten (= DSK III).

1. Nach den jeweiligen Datenschutzklassen erforderliche Maßnahmen

Die zum Schutz der Daten erforderlichen Maßnahmen richten sich nach der Einordnung in eine von drei Datenschutzklassen (vgl. KDO-DVO IV. Anlage 2 zu § 6 KDO Pkt. 4.1-4.3). Die jeweils erforderlichen Maßnahmen sind auch bei Auftragsdatenverarbeitung einzuhalten; die Kontrollierbarkeit der Durchführung der Maßnahmen durch den Auftraggeber ist sicherzustellen.

2. Maßnahmen in den Datenschutzklassen

2.1 Maßnahmen in Datenschutzklasse I

Zum Schutz der in die Datenschutzklasse I einzuordnenden Daten ist ein Schutzniveau I zu definieren. Dieses setzt mindestens voraus:

- Der Arbeitsplatzcomputer (APC) ist nicht frei zugänglich, z. B. in einem abschließbaren Gebäude oder unter ständiger Aufsicht.
- Die Anmeldung am APC ist nur nach Eingabe eines benutzerdefinierten Kennwortes möglich.
- Sicherungskopien der Datenbestände sind verschlossen aufzubewahren.
- Vor der Weitergabe eines Datenträgers für einen anderen Einsatzzweck sind die auf ihm befindlichen Daten so zu löschen, dass ihre Wiederherstellung ausgeschlossen ist.
- Nicht öffentlich verfügbare Daten sind nur dann weiterzugeben, wenn sie durch geeignete Schutzmaßnahmen geschützt sind. Die Art und Weise des Schutzes ist vor Ort zu definieren.

2.2 Maßnahmen in Datenschutzklasse II

Zum Schutz der in die Datenschutzklasse II einzuordnenden Daten ist ein Schutzniveau II zu definieren. Dieses setzt mindestens voraus, dass neben dem Schutzniveau I mindestens folgende Voraussetzungen gegeben sind:

- Die Anmeldung am APC ist nur nach Eingabe eines benutzerdefinierten Kennwortes möglich, dessen Erneuerung in regelmäßigen Abständen systemseitig vorgesehen werden muss.
- Das Laden des Betriebssystems der Datenverarbeitungsanlage darf nur mit dem dafür bereitgestellten Betriebssystem erfolgen (Bootschutz). Diese BIOS-Einstellung ist durch ein besonderes Passwort zu sichern, das nur dem Systemverwalter bekannt ist.
- Im Mehrbenutzer- oder Netzwerkbetrieb und bei einer PC/Host-Koppelung ist eine abgestufte Rechteverwaltung erforderlich. Der Anwender sollte keine Administrationsrechte erhalten.
- Sicherungskopien und Ausdrücke der Datenbestände sind vor Fremdzugriff und vor der gleichzeitigen Vernichtung mit den Originaldaten zu schützen.
- Die Daten der Schutzklasse II sind auf zentralen Systemen in besonders gegen unbefugten Zutritt gesicherten Räumen zu speichern, sofern keine begründeten Ausnahmefälle gegeben sind. Die jeweils beteiligten Systeme und Transportwege sind nach dem aktuellen Stand der Technik angemessen zu schützen.
- Eine Speicherung auf mobilen Datenträgern darf nur erfolgen, wenn diese mit einem geeigneten Zugriffsschutz ausgestattet sind.

2.3 Maßnahmen in Datenschutzklasse III

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:

Soweit es unvermeidlich ist, dass Daten der Datenschutzklasse III auf mobilen Geräten und Datenträgern gespeichert werden müssen, sind diese Daten verschlüsselt abzuspeichern. Das Verschlüsselungsverfahren ist nach dem aktuellen Stand der Technik angemessen auszuwählen.

Besonderes Augenmerk muss dabei auf langfristige und nutzerunabhängige Lesbarkeit der zu speichernden Daten gelegt werden. So müssen z. B. bei verschlüsselten Daten die Sicherheit des Schlüssels und die erforderliche Entschlüsselung auch im Datensicherungskonzept berücksichtigt werden.

Anm.: Dies gilt nicht für die Festplatten von Druckern, sofern sichergestellt ist, dass diese nicht von einem Benutzerarbeitsplatz ausgelesen werden können.

3. Maßnahmen zur Datensicherung

Der Dienststellenleiter ist für die Erstellung und Umsetzung eines Datensicherungskonzeptes verantwortlich. Besonderes Augenmerk muss dabei auf die langfristige und nutzerunabhängige Lesbarkeit der zu speichernden Daten in der Datensicherung gelegt werden.

Zum Schutz des personenbezogenen Datenbestandes vor dessen Verlust sind regelmäßige Datensicherungen erforderlich. Dabei sind u. a. folgende Aspekte mit zu berücksichtigen:

3.1 Sicherungskopien der verwendeten Programme

Es sind Sicherungskopien der verwendeten Programme in allen verwendeten Versionen anzulegen und möglichst von den Originaldatenträgern der Programme und den übrigen Datenträgern getrennt aufzubewahren.

3.2 Zeitabstände bei der Datensicherung

Die Datensicherung soll in Umfang und Zeitabstand anhand der entstehenden Auswirkungen eines Verlustes der Daten festgelegt werden.

4. Besondere Gefahrenlagen

4.1 Fernwartung

Eine Fernwartung von APC durch externe Unternehmer schafft besondere Gefahren hinsichtlich der Ausspähung von Daten. Sie darf daher nur erfolgen, wenn der Beginn aktiv seitens des Auftraggebers eingeleitet wurde und der Verlauf sowie das Ende mindestens überprüfbar sind.

4.2 Auftragsdatenverarbeitung

Eine Speicherung von Daten in PublicCloud-Systemen ist grundsätzlich untersagt. Ausnahmen bedürfen einer ausdrücklichen Genehmigung durch den Generalvikar.

4.3 Nutzung privater Datenverarbeitungssysteme

Werden im zu genehmigenden Einzelfall personenbezogene Daten auf privaten Datenverarbeitungsanlagen verarbeitet oder werden personenbezogene Daten auf private E-Mail-Konten geleitet, sind die Nutzer schriftlich auf die Einhaltung dieser IT-Richtlinie zu verpflichten. In dieser Erklärung verpflichten sich die Nutzer, betreffende personenbezogene Daten durch die Dienststelle und auf deren Anforderung löschen zu lassen. Ergänzend soll dem Nutzer eine spezifische Handlungsanleitung ausgehändigt werden, um den Schutz dieser Daten zu gewährleisten. Die Nutzung sonstiger E-Mail-Accounts für dienstliche Zwecke und die automatische Weiterleitung der dienstlichen E-Mails auf sonstige E-Mail-Accounts ist nicht gestattet (vgl. Dienstanweisung zur Benutzung dienstlicher E-Mail-Adressen im Würzburger Diözesanblatt 160 (2014) Nr. 2 vom 03.02.2014).

Der Dienststelle wird das Recht eingeräumt, die gespeicherten dienstlichen Daten aus wichtigem Grund auch ohne Einwilligung des Nutzers zu löschen und, falls dies unumgänglich ist, die auf dem APC gespeicherten privaten Daten zu löschen.

4.4 Wartungsarbeiten in der Dienststelle durch externe Auftragnehmer

Bei der Durchführung von Wartungsarbeiten innerhalb der Dienststelle ist mit besonderer Sorgfalt darauf zu achten und nach Möglichkeit auch technisch sicherzustellen, dass keine Kopien der personenbezogenen Datenbestände gefertigt werden können. Muss dem Wartungsdienst bei Vornahme der Arbeiten ein Passwort mitgeteilt werden, ist dieses sofort nach deren Beendigung zu ändern.

4.5 Wartungsarbeiten außerhalb der Dienststelle

Die Durchführung von Wartungsarbeiten in den Räumen eines Fremdunternehmens auf Datenträgern mit Daten der DSK III sollte nur in besonderen Ausnahmefällen erfolgen. Das Fremdunternehmen ist vor Beginn der Wartungsarbeiten auf die Einhaltung der KDO zu verpflichten.

4.6 Verschrottung und Vernichtung von Datenträgern

Es sind Maßnahmen bei der Verschrottung bzw. Vernichtung von Datenträgern zu ergreifen, die die Lesbarkeit oder Wiederherstellbarkeit der Datenträger zuverlässig ausschließen.

4.7 Passwortlisten der Systemverwaltung

Der Systemverwalter muss alle nicht zurücksetzbaren Passwörter (z. B. BIOS- und Administrationspasswörter) besonders gesichert aufbewahren.

5. Inkrafttreten

Diese IT-Richtlinien treten zum 1. November 2015 in Kraft.

Würzburg, 12. Oktober 2015

Thomas Keßler
Generalvikar

Bekanntmachungen

Seelsorge

Zählung der sonntäglichen Gottesdienstteilnehmer

am 8. November 2015

Gemäß Beschlüssen der Deutschen Bischofskonferenz (vgl. Vollversammlung vom 24.-27. Februar 1969, Prot. Nr. 18, und Ständiger Rat vom 27. April 1992, Prot. Nr. 5) werden für die Zwecke der kirchlichen Statistik der Bistümer in der Bundesrepublik Deutschland die Gottesdienstteilnehmer zwei Mal im Jahr gezählt. Die zweite Zählung findet einheitlich am zweiten Sonntag im November (8. November 2015) statt. Zu zählen sind alle Personen, die an den sonntäglichen Hl. Messen (einschließlich Vorabendmesse) teilnehmen. Mitzuzählen sind auch die Besucher der Wort- oder Kommuniongottesdienste, die anstelle einer Eucharistiefeier gehalten werden. Zu den Gottesdienstteilnehmern zählen auch die Angehörigen anderer Pfarreien (z. B. Wallfahrer, Seminarteilnehmer, Touristen und Besuchsreisende).

Das Ergebnis dieser Zählung ist am Jahresende in den Erhebungsbogen der kirchlichen Statistik für das Jahr 2015 unter der Rubrik „Gottesdienstteilnehmer am zweiten Sonntag im November“ (Pos. 3) einzutragen.