Erzbischöfliches Generalvikariat

Verordnung

9. Anordnung über den kirchlichen Datenschutz (KDO)

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 Anordnung erlassen:

§ 1
Zweck und Anwendungsbereich

(1) Zweck dieser Anordnung ist es, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Diese Anordnung gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten in Dateien 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) Bei der Anwendung dieser Anordnung gelten folgende Einschränkungen:

1. Für automatisierte Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt werden und nach ihrer verarbeitungstechnischen Nutzung automatisch gelöscht werden, gelten nur die §§ 4 und 6.

2. Für nicht automatisierte Dateien, deren personenbezogene Daten nicht zur Übermittlung an Dritte bestimmt sind, gelten nur die §§ 4 und 6. Werden im Einzelfall personenbezogene Daten übermittelt, gelten für diesen Einzelfall die Vorschriften dieser Anordnung uneingeschränkt.

(4) Soweit besondere kirchliche oder staatliche Rechtsvorschriften auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieser Anordnung 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) Eine Datei ist

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder

2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht-automatisierte Datei).

Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, daß sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

(3) Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(4) Erheben ist das Beschaffen von Daten über den Betroffenen.

(5) 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 (Empfänger) in der Weise, daß
   a) die Daten durch die speichernde Stelle an den Empfänger weitergegeben werden oder
   b) der Empfänger von der speichernden Stelle zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(6) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(7) 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 bestimmbaren natürlichen Person zugeordnet werden können.

(8) Speichernde Stelle ist jede in § 1 Abs. 2 genannte Stelle, die personenbezogene Daten für sich selbst speichert oder durch andere im Auftrag speichern läßt.

(9) Dritter ist jede Person oder Stelle außerhalb der speichernden Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Geltungsbereich dieser Anordnung personenbezogener Daten im Auftrag verarbeiten oder nutzen.

§ 3
Zulässigkeit der Datenverarbeitung und -nutzung

(1) Die Verarbeitung personenbezogener Daten und deren Nutzung sind nur zulässig, soweit

1. diese Anordnung 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 Speicherung und einer vorgesehenen Übermittlung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung 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 2 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
Datengeheimnis

Den bei der Datenverarbeitung tätigen Personen ist untersagt, personenbezogene Daten unbefugt 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 in einer Datei gespeichert, bei der mehrere Stellen speicherungsberechtigt sind und ist der Betroffene nicht in der Lage, die speichernde Stelle festzustellen, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die speichernde Stelle weiterzuleiten. Der Betroffene ist über die Weiterleitung und die speichernde Stelle zu unterrichten.

§ 6
Technische und organisatorische Maßnahmen

Kirchliche Stellen im Geltungsbereich des § 1 Abs. 2, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieser Anordnung, insbesondere die in der Anlage zu dieser Anordnung 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. Datenempfänger,
3. Art der zu übermittelnden Daten,
4. nach § 6 erforderliche technische und organisatorische Maßnahmen.

(3) Über die Einrichtung von Abrufverfahren ist der Beauftragte für den Datenschutz unter Mitteilung der Festlegungen des Abs. 2 zu unterrichten.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Empfänger. 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 aus Datenbeständen, die jedermann, sei es ohne oder nach besonderer Zulassung, zur Benutzung offenstehen.

§ 8
Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieser Anordnung 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 die Datenverarbeitung (§ 2 Abs. 5) oder -nutzung (§ 2 Abs. 6), die technischen und organisatorischen Maßnahmen (§ 6) und etwaige Unterauftragsverhältnisse festzulegen sind.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten oder nutzen. Ist er der Ansicht, daß eine Weisung des Auftraggebers gegen diese Anordnung oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

§ 9
Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden 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 mit seiner Kenntnis erhoben, so ist der Erhebungszweck ihm gegenüber anzugeben. 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. 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.

§ 10
Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der speichernden 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,
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 aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist,

7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Straftaten oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßregeln 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.

(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 speichernde Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die speichernde 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.

§ 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 des Empfängers 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 des Empfängers, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des

Empfängers liegt, es sei denn, daß besonderer Anlaß zur Prüfung der Zulässigkeit der Übermittlung besteht. § 7 Abs. 4 bleibt unberührt.

(3) Der Empfänger darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm 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 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 unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte 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 und nicht-öffentliche Stellen 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 Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) In den Fällen der Übermittlung nach Abs. 1 Ziff. 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 oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder dem kirchlichen Wohl Nachteile bereiten würde.

(4) Der Empfänger darf die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat den Empfänger darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Abs. 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 Herkunft oder Empfänger dieser Daten beziehen und
2. 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 in Akten gespeichert (§ 2 Abs. 2 Nr. 1), 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 von dem 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, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen.

(3) Die Auskunfterteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der speichernden 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 Beauftragten für den Datenschutz wenden kann.

(5) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Beauftragten für den Datenschutz zu erteilen, soweit nicht das Bistum im Einzelfall feststellt, daß dadurch das kirchliche Wohl beeinträchtigt wird. Die Mitteilung des Beauftragten für den Datenschutz an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(6) Die Auskunft ist unentgeltlich.

§ 14
Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, daß personenbezogene Daten in Akten unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.

(2) Personenbezogene Daten in Dateien sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die speichernde 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 in Dateien sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt.

(5) Personenbezogene Daten in Akten sind zu sperren, wenn die speichernde Stelle im Einzelfall feststellt, daß ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der speichernden Stelle nicht mehr erforderlich sind.

(6) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen, im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist und die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

(7) 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 regelmäßigen Datenübermittlung diese Daten zur Speicherung weitergegeben werden, wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist.

§ 15
Anrufung des Beauftragten für den Datenschutz

Jedermann kann sich an den Beauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch Stellen gemäß § 1 Abs. 2 in seinen Rechten verletzt worden zu sein.

§ 16
Bestellung und Rechtsstellung des Beauftragten für den Datenschutz

(1) Der Bischof bestellt für den Bereich seines Bistums einen Beauftragten für den Datenschutz. Die Bestellung erfolgt für die Dauer von drei Jahren. Wiederbestellung ist möglich. Bei Vorliegen eines wichtigen Grundes kann der Bischof vorzeitig die Bestellung zurücknehmen. Auf Antrag des Beauftragten nimmt der Bischof die Bestellung zurück.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Er ist auf die gewissenhafte Erfüllung seiner Pflichten und die Einhaltung des kirchlichen und des für die Kirchen verbindlichen staatlichen Rechts zu verpflichten.

(3) Der Beauftragte für den Datenschutz ist in Ausübung seiner Tätigkeit unabhängig und nur dem kirchlichen Recht und dem für die Kirchen verbindlichen staatlichen Recht unterworfen.

(4) Der Beauftragte für den Datenschutz ist, auch nach Beendigung seines Auftrages, verpflichtet, über die ihm in seiner Eigenschaft als Beauftragter für den Datenschutz 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.

(5) Der Beauftragte für den Datenschutz 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.

§ 17
Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz wacht über die Einhaltung der Vorschriften dieser Anordnung 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 Beauftragte für den Datenschutz Gutachten zu erstellen und Berichte zu erstatten.

(2) Die in § 1 Abs. 2 genannten Stellen sind verpflichtet, den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen. 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 Beauftragte für den Datenschutz führt ein Register der automatisch betriebenen Dateien, in denen personenbezogene Daten gespeichert werden. Das Register kann von jedermann eingesehen werden. Die in § 1 Abs. 2 genannten Stellen sind verpflichtet, die von ihnen automatisch betriebenen Dateien beim zuständigen Beauftragten für den Datenschutz anzumelden.

(4) Der Beauftragte für den Datenschutz wirkt auf die Zusammenarbeit mit den kirchlichen Stellen, insbesondere mit den anderen kirchlichen Beauftragten für den Datenschutz, hin.

(5) Zu seinem Aufgabenbereich gehört die Zusammenarbeit mit den staatlichen Beauftragten für den Datenschutz.

§ 18
Beanstandungen durch den Beauftragten für den Datenschutz

(1) Stellt der Beauftragte für den Datenschutz Verstöße gegen die Vorschriften dieser Anordnung oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er diese gegenüber der zuständigen aufsichtsführenden Stelle und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf.

(2) Der Beauftragte für den Datenschutz kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, wenn es sich um unerhebliche Mängel handelt.

(3) Mit der Beanstandung kann der Beauftragte für den Datenschutz Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die gem. Abs. 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandungen des Beauftragten für den Datenschutz getroffen worden sind.

§ 19
Ermächtigungen

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

a) den Inhalt der schriftlichen Verpflichtungserklärung gemäß § 4 Satz 2,

b) die technischen und organisatorischen Maßnahmen gemäß § 6 Satz 1,

c) den Inhalt der Anmeldung gemäß § 17 Abs. 3 Satz 3.

§ 20
Schlußbestimmung

Diese Anordnung tritt am 1.1.1994 in Kraft.

Gleichzeitig tritt die Anordnung über den Kirchlichen Datenschutz (KDO) vom 1.7.1978 bzw. vom 1.1.1979 (vgl. Amtsblatt 1978, S. 254–264) außer Kraft.

Anlage zu § 6 dieser Anordnung

Werden personenbezogene Daten automatisch verarbeitet, sind zur Ausführung der Vorschriften dieser Anordnung Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

(1) Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),

(2) Personen, die bei der Verarbeitung personenbezogener Daten tätig sind, daran zu hindern, daß sie Datenträger unbefugt entfernen (Abgangskontrolle),

(3) die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),

(4) die Benutzung von Datenverarbeitungssystemen, aus denen oder in die personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden, durch unbefugte Personen zu verhindern (Benutzerkontrolle),

(5) zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten durch selbsttätige Einrichtungen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),

(6) zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden können (Übermittlungskontrolle),

(7) zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),

(8) zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

(9) zu gewährleisten, daß bei der Übermittlung personenbezogener Daten sowie beim Transport entsprechender Datenträger diese nicht unbefugt gelesen, verändert oder gelöscht werden können (Transportkontrolle),

(10) die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

Dr. Robert Simon, Generalvikar Dr. Modesto