

**Anordnung**  
**über den Kirchlichen Datenschutz**  
**– KDO –**  
**in der Diözese Hildesheim**

**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 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 durch:
  1. das Bistum, die Kirchengemeinden, die Kirchenstiftungen und die Kirchengemeinerverbände,
  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 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) 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 bestimmbar 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 Anordnung personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.
- (10) Besondere Arten personenbezogener Daten sind Angaben über die rassische 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 ausübende oder eine andere Stelle automatisiert verarbeitet werden können und
  3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

## § 2a

### **Datenvermeidung und Datensparsamkeit**

Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung

zung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

### § 3

#### **Zulässigkeit der Datenerhebung, -verarbeitung oder -nutzung**

- (1) Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist 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 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.

### § 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 § 18 a bestellt wurde oder bei ihr höchstens zehn Personen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betraut sind.
- (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 (Videüberwachung) ist nur zulässig, soweit sie
  1. zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts oder
  2. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich 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 § 13 a 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 Maßnahmen unterrichten, 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 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. 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 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 Datenerhebung (§ 2 Abs. 3), Datenverarbeitung (§ 2 Abs. 4) oder -nutzung (§ 2 Abs. 5), die technischen und organisatorischen Maßnahmen (§ 6) und etwaige Unterauftragsverhältnisse festzulegen sind. Der Auftraggeber hat sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.
- (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 Anordnung 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 denn, 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,

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, oder
  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.

## § 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 Übermittlungersuchen 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 unverhältnismäßigem 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**

Jedermann kann sich an den Diözesandatenschutzbeauftragten 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 Diözesandatenschutzbeauftragten**

- (1) Der Bischof bestellt für den Bereich seines Bistums einen Diözesandatenschutzbeauftragten. 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 Diözesandatenschutzbeauftragten 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 Diözesandatenschutzbeauftragte ist in Ausübung seiner Tätigkeit unabhängig und nur dem kirchlichen Recht und dem für die Kirchen verbindlichen staatlichen Recht unterworfen.
- (4) Der Diözesandatenschutzbeauftragte ist, auch nach Beendigung seines Auftrages, verpflichtet, über die ihm in seiner Eigenschaft als Diözesandatenschutzbeauftragtem bekannten 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 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.

## **§ 17**

### **Aufgaben des Diözesandatenschutzbeauftragten**

- (1) Der Diözesandatenschutzbeauftragte 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 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 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 Diözesandatenschutzbeauftragte erstattet dem Bischof alle 3 Jahre einen Tätigkeitsbericht. 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.

## **§ 18**

### **Beanstandungen durch den Diözesandatenschutzbeauftragten**

- (1) Stellt der Diözesandatenschutzbeauftragte 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 Diözesandatenschutzbeauftragte 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 Diözesandatenschutzbeauftragte 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 Diözesandatenschutzbeauftragten getroffen worden sind.

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

## **§ 18a**

### **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) 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.
- (3) 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.
- (4) Die kirchlichen Stellen haben den betrieblichen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Betroffene können sich jederzeit an den betrieblichen Datenschutzbeauftragten wenden.
- (5) Im Übrigen findet § 16 entsprechende Anwendung.

## **§ 18b**

### **Aufgaben des betrieblichen Datenschutzbeauftragten**

- (1) Der betriebliche Datenschutzbeauftragte wirkt auf die Einhaltung dieser Anordnung und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann er sich in Zweifelsfällen an den Diözesandatenschutzbeauftragten gemäß § 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 Anordnung 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 § 3 a Abs. 2 zur Verfügung zu stellen.
- (3) Der betriebliche Datenschutzbeauftragte macht die Angaben nach § 3 a Abs. 2 Nr. 1 bis 7 auf Antrag jedermann in geeigneter Weise verfügbar, der ein berechtigtes Interesse nachweist.

## **§ 19**

### **Ermächtigungen**

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

- a) den Inhalt der Meldung gemäß § 3 a
- b) den Inhalt der schriftlichen Verpflichtungserklärung gem. § 4 Satz 2,
- c) die technischen und organisatorischen Maßnahmen gem. § 6 Satz 1.

## **§ 20**

### **Schlussbestimmung**

Diese Anordnung tritt am 01. November 2003 in Kraft.

Gleichzeitig tritt die Anordnung über den kirchlichen Datenschutz – KDO – vom 01.01.1994 außer Kraft.

Hildesheim, den 15. Oktober 2003

† Josef  
Bischof von Hildesheim

## **Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO) in der Diözese Hildesheim**

Aufgrund des § 19 der Anordnung über den kirchlichen Datenschutz (KDO) vom 01.11.2003 werden mit Wirkung vom 01.11.2003 die folgenden Regelungen getroffen:

### **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 § 3a 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,
  4. 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 Abschnitt III KDO-DVO zu verwenden.

#### **IV. Anlage 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.

#### **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 § 13a 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.**

Die Verordnung zur Durchführung der Anordnung über den Kirchlichen Datenschutz (KDO-DVO) vom 30. Juni 1994 tritt hiermit außer Kraft.

Hildesheim, den 15. Oktober 2003

Bernert  
Generalvikar

## **Anlagen**

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

*Die Notwendigkeit für die in dem nachfolgenden Formular (Muster 1) 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 aus.*

Muster

## Meldung von Verfahren automatisierter Verarbeitungen

- Ersterfassung**
- Änderung/Ergänzung**

Dieses Formular ist auszufüllen aufgrund Abschnitt I der KDO-DVO (§3a KDO) und dem Diözesandatenschutzbeauftragten zu melden, sofern kein betrieblicher Datenschutzbeauftragter bestellt ist.

**Rechtsträger** (§ 1 Abs. 2 KDO) (z.B. Kirchengemeinde)

---

Name, Anschrift (evtl. Stempel)

- 1. Verantwortliche 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 Kirchengemeinde)

---

Name, Anschrift (evtl. Stempel)

- 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 Kirchengemeinde)

---

Name

2.2 mit der Leitung der Datenverarbeitung in der verantwortlichen Stelle beauftragte Personen (z.B. beauftragte Gruppenleiterin im Kindergarten der Kirchengemeinde)

---

Name, Telefonnummer

- 3. Aufgaben, zu deren Erfüllung die Kenntnis der Daten erforderlich ist. (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. Meldedaten, Personaldaten, aus. So genannte „besondere Arten personenbezogener Daten“ (vgl. § 2 Abs. 10 KDO) sind entsprechend anzugeben.)

---

---

---

---

---

#### **5. Empfänger oder Kategorien von Empfänger, denen die Daten mitgeteilt werden können (jede Person oder Stelle, die Daten erhält [§ 2 Abs. 9 KDO])**

(z.B. Behörden, kirchliche Stellen, Versicherungen, ärztl. Personal usw.)

---

---

---

---

---

**6. Regelfristen für die Löschung der Daten**

---

---

---

---

**7. Geplante Datenübermittlung ins Ausland**

---

---

**8. Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung**

(z.B. Konfigurationsübersicht, Netzwerkstruktur, Betriebs- und Anwendersoftware, spezielle Sicherungssoftware usw.) (Evtl. gesonderte Aufstellung)

---

---

---

---

---

**9. Zugriffsberechtigte Personen**

---

---

---

---

---

Ort, Datum, Unterschrift

2.) Zu Abschnitt III. KDO-DVO (§ 4 Satz 2 KDO)  
Muster 1

**Verpflichtungserklärung**  
**gemäß § 4**  
**der Anordnung über den kirchlichen Datenschutz**  
**- KDO -**

Ich, \_\_\_\_\_  
(Vor- und Zuname)

geb. am \_\_\_\_\_

wohnhaft in \_\_\_\_\_  
\_\_\_\_\_

bin bei/in \_\_\_\_\_ tätig.

Ich verpflichte mich,

1. die Anordnung über den kirchlichen Datenschutz - KDO - des Bistums Hildesheim sowie die anderen für meine Tätigkeit geltenden Datenschutzregelungen einschließlich der zu ihrer Durchführung ergangenen Bestimmungen in der jeweils geltenden Fassung sorgfältig einzuhalten und 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 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 die KDO und andere für meine Tätigkeit geltenden Datenschutzvorschriften disziplinarrechtliche beziehungsweise arbeitsrechtliche/rechtliche Folgen haben kann.

Diese Erklärung wird zu meiner Personalakte genommen.

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Unterschrift (Vor- und Zuname)

**Verpflichtungserklärung  
für Ehrenamtliche  
gemäß § 4  
der Anordnung über den kirchlichen Datenschutz  
- KDO -**

Ich, \_\_\_\_\_  
(Vor- und Zuname)

geb. am \_\_\_\_\_

wohnhaft in \_\_\_\_\_  
\_\_\_\_\_

bin bei/in \_\_\_\_\_ ehrenamtlich tätig.

Ich verpflichte mich,

alle datenschutzrechtlichen Bestimmungen des Bistums Hildesheim einzuhalten und alle personenbezogenen Angaben, die ich aufgrund meines Ehrenamtes erhalten habe oder die mir im Zusammenhang mit meinem Ehrenamt zur Kenntnis gelangt sind, während der Tätigkeit und nach ihrer Beendigung vertraulich zu behandeln. Ich bin darüber informiert, dass Verstöße gegen das Datengeheimnis zum Entzug des Ehrenamtes führen können. Auf mögliche Schadenersatzansprüche einer unzulässigen Weitergabe personenbezogener Daten wurde ich hingewiesen.

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Unterschrift (Vor- und Zuname)

## **Das neue kirchliche Datenschutzrecht**

Am 01. November 2003 sind eine neue Anordnung über den kirchlichen Datenschutz - KDO - sowie eine neue Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO) in Kraft getreten, die die neun Jahre alten Bestimmungen aus dem Jahre 199... abgelöst haben. Damit verbunden sind eine Vielzahl wesentlicher Änderungen und Neuerungen. Alle Mitarbeiterin unseren Dienststellen und Einrichtungen, die mit der Verarbeitung personenbezogener Daten zu tun haben, müssen die neuen Vorschriften beachten und täglich in der Praxis anwenden. Um ihnen diese Aufgabe zu erleichtern sollen hier einige erste wichtige Hinweise gegeben werden.

### **Anlass zur Schaffung der neuen KDO**

Durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 (Abl. EG Nr. L 281, Seite 31 ff.) wurden einheitliche Mindestanforderungen an den Datenschutz in den Mitgliedsstaaten der Europäischen Union geschaffen. Im Hinblick hierauf haben der Bund und die Länder ihr Datenschutzrecht reformiert und sowohl das Bundesdatenschutzgesetz (BDSG), wie auch die Landesdatenschutzgesetze jeweils vollständig neu gefaßt. Dem Selbstverwaltungsrecht der öffentlich-rechtlichen Religionsgesellschaften wurde weiterhin dadurch Rechnung getragen, dass kirchliche Einrichtungen nicht in den Regelungsbereich dieser Gesetze einbezogen wurden. Hierin lag Verpflichtung und Ansporn zugleich, nun durch eine eigene Reform, zur Umsetzung der europäischen Standards und zur Fortentwicklung des Datenschutzrechts beizutragen.

### **Materielle Änderungen**

#### 1. Neue Begriffe

Die Anpassung an das europäische Recht hat im Hinblick auf den Sprachgebrauch in den europäischen Staaten eine Änderung der Begriffsdefinitionen des § 2 KDO mit sich gebracht:

- a) So spricht § 2 Abs. 2 KDO jetzt von *automatisierter Verarbeitung* und nicht mehr von *automatisierten Dateien*, mit der Folge, dass jetzt auch Videoaufzeichnungen hierunter fallen, die bisher Bestandteil von Akten waren (§ 2 Abs. 3 KDO-1994). Neben den EDV- und Videoüberwachungsanlagen gehören auch Textverarbeitungssysteme zu den „Datenverarbeitungsanlagen“ i.S. dieser Vorschrift. Die Begriffe *Akten* und *Aktensammlungen* sind entfallen.
- b) Neu eingefügt wurde der Begriff *Pseudonymisieren* (§ 2 Abs. 7 KDO).
- c) Aus der *speichernden Stelle* ist jetzt die *verantwortliche Stelle* geworden (§ 2 Abs. 8 KDO).
- d) *Besondere Arten personenbezogener Daten* (§ 2 Abs. 10 KDO) sind auf Grund ihrer Sensibilität geeignet, das informationelle Selbstbestimmungsrecht der Betroffenen in hohem Maße zu gefährden. Daher besteht für sie ein generelles Verbot, das jedoch von einer Reihe von Ausnahmen durchbrochen wird (§ 9 Abs. 5 KDO)
- e) § 2 Abs. 11 KDO enthält jetzt eine Definition für *mobile personenbezogene Speicher- und Verarbeitungsmedien* (Chipkarten). Diese haben in den letzten Jahren zunehmend an Be-

deutung gewonnen. Auch im kirchlichen Bereich gibt es Überlegungen zu ihrer Einführung (Church-Card). Es war daher konsequent, sie frühzeitig in den Regelungsbereich der KDO (§ 5b KDO) mit einzubeziehen.

## 2. Grundsatz der Datenvermeidung und Datensparsamkeit (§ 2a KDO)

Neu aufgenommen wurde der Grundsatz der Datenvermeidung und Datensparsamkeit. Er ergänzt den Grundsatz der Erforderlichkeit (§§ 9 Abs.1, 10 Abs. 1 KDO) um eine technische Komponente. Durch eine entsprechende Gestaltung der Datenverarbeitungssysteme soll den Gefahren für das informationelle Selbstbestimmungsrecht schon zu einem möglichst frühen Zeitpunkt begegnet werden. Die pseudonymisierte (§ 2 Abs. 7 KDO) und anonymisierte (§ 2 Abs. 6 KDO) Verarbeitung hat, wo immer möglich, den Vorrang.

## 3. Regelung zur Videoüberwachung (§ 5a KDO)

Vom neuen BDSG wurden auch die Regelungen zur Videoüberwachung, die inzwischen auch im kirchlichen Bereich große Bedeutung erlangt hat, übernommen. Die Vorschrift erfasst nur die Beobachtung öffentlich zugänglicher Räume, die von jedermann betreten werden können (z.B. Kirchen, Flure und Stationen in Krankenhäusern, Vorplätze von Gebäuden, etc.). Für die Überwachung ausschließlich intern zugänglicher Räume (z.B. Arbeitszimmer) gelten weiterhin die Grundsätze des Arbeitnehmerdatenschutzes.

Die Regelung ist im Grunde zwar sehr weit gefasst, bietet aber eine Reihe von Vorteilen. So zwingt sie die überwachende Stelle zu einer präzisen Begründung der Maßnahme im Hinblick auf die damit verbundenen Ziele. Dabei stellt sich nicht selten heraus, dass die Überwachungsmaßnahme allein für sich gesehen noch keinen ausreichenden Schutz bietet. Zudem ist die Tatsache der Überwachung in geeigneter Form kenntlich zu machen. Für verdeckte Überwachungsmaßnahmen bietet § 5a KDO keine Rechtsgrundlage.

## 4. Stärkung der Rechte der Betroffenen

Betroffene müssen sich zwar in vielen Fällen eine Verarbeitung ihrer personenbezogenen Daten durch kirchliche Dienststellen und Einrichtungen gefallen lassen, haben dem gegenüber jedoch auch eine Reihe von Rechten zur Wahrung ihres informationellen Selbstbestimmungsrechts.

- Zunächst haben sie das Recht, dass die Daten, von Ausnahmefällen abgesehen, bei ihnen selbst erhoben werden (§ 9 Abs. 2 KDO)
- In vielen Fällen ist hierzu ihre *Einwilligung* erforderlich (§ 3 Abs. 1, 3, 5 KDO).
- Werden die Daten nicht unmittelbar beim Betroffenen erhoben, so besteht eine *Benachrichtigungspflicht* (§ 13a KDO).
- In jedem Fall hat er das Recht auf *Auskunft* (§ 13 KDO) auf die zu seiner Person gespeicherten Daten, ihre Herkunft, ihre Weitergabe und den Zweck der Speicherung. Nur in schwerwiegenden Fällen kann ihm diese verweigert werden (§ 13 Abs. 3 KDO).
- Wie bisher kann er auch die *Berichtigung* (§ 14 Abs. 1 KDO) unrichtiger Daten, die *Löschung* (§ 14 Abs. 2 KDO) nicht mehr benötigter Daten und die *Sperrung* (§ 14 Abs. 3, 4 KDO) von Daten, deren Richtigkeit von ihm bestritten wurde, oder die nur auf Grund von Aufbewahrungsvorschriften nicht gelöscht werden dürfen, verlangen.

- Neu geschaffen wurde das Widerspruchsrecht in § 14 Abs. 5 KDO. Erstmals kann der Betroffene damit auch einer rechtmäßigen Datenverarbeitung widersprechen. Um die Aufgabenerfüllung nicht zu gefährden, ist diese Möglichkeit jedoch für den Fall der gesetzlichen Anordnung der Datenverarbeitung ausgeschlossen. In allen anderen Fällen ist keine Rechtsgüterabwägung erforderlich, wobei jedoch auf dem Hintergrund einer rechtmäßigen Datenverarbeitung ein strenger Maßstab anzulegen ist. Die Geltendmachung des Widerspruchsrechts wird nicht durch eine zuvor erteilte Einwilligung ausgeschlossen.

## Organisatorische Änderungen

### 1. Technische und organisatorische Maßnahmen (§ 6 KDO)

Die Daten verarbeitenden Stellen haben, wie schon bisher durch *technische und organisatorische Maßnahmen* (§ 6 KDO) dafür zu sorgen, dass die Vorschriften der KDO eingehalten werden. Ziffer IV der Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO) zählt die konkret zu erfüllenden Anforderungen auf. Der Katalog wurde gegenüber der früheren Anlage zu § 6 KDO überarbeitet und um zwei Ziffern verkürzt. Wie schon oben erwähnt ist zudem bei der Gestaltung und Auswahl von Datenverarbeitungssystemen die Grundsätze der Datenvermeidung und Datensparsamkeit zu beachten.

### 2. Meldepflicht und Verzeichnis (§ 3a KDO)

An die Stelle des alten Dateienregisters nach § 17 Abs. 3 KDO-1994 ist nunmehr die Meldung nach § 3a Abs. 2 KDO-2003 getreten. Die hierbei zu machenden Angaben wurden im Vergleich zum früheren Recht konkreter gefasst. Zudem sollen sie eine bessere Vorstellung vom Umfang und den Risiken der jeweiligen automatisierten Verarbeitungen ermöglichen. Die Meldung hat **vor** der Inbetriebnahme der Verarbeitung zu erfolgen. Hierdurch wird es möglich, rechtzeitig auf mögliche Gefährdungen und etwa erforderlichen Gegenmaßnahmen hierzu, hinzuweisen und spätere teure Nachbesserungen vermeiden zu helfen. Die Meldungen sollen unter Verwendung des Musters in der Anlage zu KDO-DVO erfolgen. Ein Programm zur Abgabe der Meldung in elektronischer Form, ist in Entwicklung.

### 3. Betrieblicher Beauftragter für den Datenschutz (§§ 18a, 18b KDO)

Neu ist, dass jetzt alle Dienststellen und Einrichtungen die Möglichkeit haben, einen betrieblichen Datenschutzbeauftragten zu bestellen. In diesem Fall entfällt die Meldepflicht nach § 3a KDO gegenüber dem Diözesandatenschutzbeauftragten. Die Übersicht nach § 3a Abs. 2 KDO ist dem Betriebsbeauftragten zur Verfügung zu stellen. Durch diese Regelung soll der vom Bischof bestellte Diözesandatenschutzbeauftragte entlastet und eine schnellere und effektivere Aufsicht über die Datenverarbeitung vor Ort erreicht werden. Zumindest für größere Einrichtungen, die umfangreiche und komplexe Datenverarbeitungssysteme einsetzen und gleichzeitig mit sensiblen Daten umgehen, dürfte die Bestellung eines betrieblichen Datenschutzbeauftragten dringend geboten sein, um die organisatorischen Anforderungen nach § 6 KDO erfüllen zu können. Künftig werden vor allem zwei Aufgaben auf den betrieblichen Datenschutzbeauftragten zukommen:

Erstens: Die Begleitung der Einführung neuer oder der Umgestaltung bestehender Verfahren der automatischen Datenverarbeitung. Sein Beitrag hierzu sollte darin bestehen, die Anforderungen der Anlage zu § 6 KDO besonders in den Blick zu nehmen und gemeinschaftlich mit den übrigen Beteiligten nach datenschutzgerechten Lösungen zu suchen. Im Falle des Abschlusses einer Betriebsvereinbarung kann er eine vermittelnde Stellung zwischen Verwaltungsleitung und MAV einnehmen.

Zweitens: Die Unterweisung der Mitarbeiter zu einem datenschutzgerechten Umgang mit den bestehenden Verfahren. Diese Aufgabe kann er sowohl durch Mitwirkung an betriebsinternen Richtlinien, wie auch durch Schulungsmaßnahmen und Beratungen im Einzelfall wahrnehmen.

In jedem Fall arbeitet er auf diesem Gebiet der Verwaltungsleitung zu und dieser daher unmittelbar zu unterstellen.

#### 4. Diözesandatenschutzbeauftragter (§§ 16, 17, 18 KDO)

Der bisherige Bischöfliche Beauftragte für den Datenschutz wird nunmehr als *Diözesandatenschutzbeauftragter* bezeichnet. Die Begriffsänderung ist allein zur besseren Abgrenzung gegenüber dem betrieblichen Datenschutzbeauftragten erfolgt. Wesentliche Änderungen in seiner Rechtsstellung und seinen Aufgaben sind damit nicht verbunden. Gesetzlich festgelegt wurde jetzt, dass dieser dem Bischof alle drei Jahre einen Tätigkeitsbericht zu erstatten hat. Die Verpflichtung, den Diözesandatenschutzbeauftragten in der Erfüllung seiner Aufgaben zu unterstützen (§ 17 Abs. 2 KDO) besteht auch für die Einrichtungen, die einen betrieblichen Datenschutzbeauftragten bestellt haben. Dieser kann sich zudem jederzeit an den Diözesandatenschutzbeauftragten wenden (§ 18b Abs. 1 Satz 2 KDO). Zur Verbesserung des Datenschutzes sollte es daher in jedem Fall zu einer vertrauensvollen und intensiven Zusammenarbeit kommen.

### Was ist zu tun?

#### 1. Unterrichtung der Mitarbeiter

Die in der Datenverarbeitung tätigen Mitarbeiter sollten in geeigneter Weise mit der neuen Rechtslage vertraut gemacht werden. Hierzu sollte ihnen zumindest ein Textabdruck der neuen KDO mit diesen Hinweisen zur Verfügung gestellt werden. Bei dieser Gelegenheit sollte auch überprüft werden, ob alle Mitarbeiter die Verpflichtungserklärung nach § 4 KDO unterzeichnet haben.

#### 2. Bestellung eines betrieblichen Beauftragten für den Datenschutz

Sodann sollte in jeder Einrichtung geprüft werden, ob die Bestellung eines betrieblichen Datenschutzbeauftragten notwendig ist. Hierbei sollten folgende Aspekte geprüft werden:

- a) Welchen Umfang hat die automatisierte Datenverarbeitung in unserer Einrichtung?
- b) Sind die verarbeiteten personenbezogenen Daten von Klienten, Mitarbeitern, etc. besonders sensibel? Gehören sie zur Gruppe der besonders schützenswerten Daten i.S.v. § 2 Abs. 10 KDO?
- c) Wie groß ist das Gefährdungspotential für diese Daten? Hat es in der Vergangenheit schon Vorfälle gegeben, durch die besondere Gefährdungen sichtbar wurden (z.B. Hoch-

wassereinbrüche, Diebstahl von PC und Datenträgern, Systemabstürze mit längeren Ausfallzeiten, erfolgreiche Virenangriffe, etc.)?

- d) Wird die Organisation in unserer Einrichtung den Anforderungen der Anlage zu § 6 KDO gerecht? Sind die verwendeten Daten stets verfügbar, inhaltlich richtig und ihre Vertraulichkeit gewahrt?
- e) Hat es in der Vergangenheit häufiger Beschwerden Betroffener gegeben?

### 3. Meldung automatisierter Verfahren nach § 3a KDO

Soweit ein betrieblicher Datenschutzbeauftragter nicht bestellt wird, sind alle bestehenden und schon jetzt neu geplanten Verfahren automatisierter Verarbeitungen, wie EDV-Anlagen, Videoüberwachungsanlagen, automatisierte Textverarbeitungssysteme dem Diözesandatenschutzbeauftragten unter Verwendung des Musters in der Anlage zur KDO-DVO zu melden.

Hannover, den 18. Februar 2004  
Lutz Grammann  
Diözesandatenschutzbeauftragter

### **Wichtige Anschriften:**

- Der Diözesandatenschutzbeauftragte der (Erz-)Bistümer Berlin, Hamburg, Hildesheim, Osnabrück und Münster im oldenburgischen Teil  
Engelbosteler Damm 72 - 30167 Hannover - Phone: 0511 / 81 93 15  
Email: [info@datenschutz-kirche.de](mailto:info@datenschutz-kirche.de) - internet: <http://www.datenschutz-kirche.de>
- Datenschutzreferent im (Erz-)bischöflichen Generalvikariat / Ordinariat:  
.....
- Betrieblicher Datenschutzbeauftragter für den Diözesancaritasverband:  
.....

### **Wichtige Internetadressen:**

- Virtuelles Datenschutzbüro  
<http://www.datenschutz.de>
- Bundesamt für Sicherheit in der Informationstechnik  
<http://www.bsi.bund.de/>
- Sicherheit im Internet. Eine Seite des Bundesministeriums für Wirtschaft und Arbeit  
<http://www.sicherheit-im-internet.de/>

## **Verlängerung der Geltung bereichsspezifischer datenschutzrechtlicher Ausführungsbestimmungen zur Anordnung über den kirchlichen Datenschutz für die Diözese Hildesheim - KDO -**

Gemäß § 19 der Anordnung über den Kirchlichen Datenschutz - KDO - in der Diözese Hildesheim vom 01.11.2003 (veröffentlicht im Kirchlichen Anzeiger für das Bistum Hildesheim, Jahrgang 2003, Seite 215 ff.) treffe ich hiermit folgende Regelung:

1. Auf der Grundlage der KDO vom 01.01.1994 (veröffentlicht im Kirchlichen Anzeiger für das Bistum Hildesheim, Jahrgang 1994, Seite 13 ff.) hatte der damalige Herr Generalvikar folgende bereichsspezifische datenschutzrechtliche Ausführungsbestimmungen zur KDO erlassen:
  - a) Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche vom 12.12.1988 (veröffentlicht im Kirchlichen Anzeiger für das Bistum Hildesheim, Jahrgang 1988, Seite 391 ff.) sowie die Empfehlung der Deutschen Bischofskonferenz zur Vervielfältigung von Pfarrmatrikeln und kirchlichen Archivarien vom 26.08.1974.
  - b) Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Hildesheim vom 01.09.1989 (veröffentlicht im Kirchlichen Anzeiger für das Bistum Hildesheim, Jahrgang 1989, Seite 204 ff.).
  - c) Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Hildesheim vom 01.04.1990 (veröffentlicht im Kirchlichen Anzeiger für das Bistum Hildesheim, Jahrgang 1990, Seite 80 ff.).
  - d) Datenschutz bei der Übermittlung personenbezogener Daten über Telefax vom 01.11.1992 (veröffentlicht im Kirchlichen Anzeiger für das Bistum Hildesheim, Jahrgang 1992, Seite 260 ff.).
  - e) Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft vom 01.01.1992 (veröffentlicht im Kirchlichen Anzeiger für das Bistum Hildesheim, Jahrgang 1992, Seite 305 ff.).
  - f) Besonderer Schutz von Computerprogrammen nach dem Urheberrechtsgesetz vom 01.10.1993 (veröffentlicht im Kirchlichen Anzeiger für das Bistum Hildesheim, Jahrgang 1994, Seite 49 ff.).
  - g) Richtlinien für den Einsatz von Informationstechnik sowie den Datenschutz am Arbeitsplatz in der Diözese Hildesheim vom 01.11.1994 (veröffentlicht im Kirchlichen Anzeiger für das Bistum Hildesheim, Jahrgang 1994, Seite 126 ff.).
  - h) Richtlinien zum Einsatz von Arbeitsplatzcomputern in der Diözese Hildesheim vom 01.11.1994 (veröffentlicht im Kirchlichen Anzeiger für das Bistum Hildesheim, Jahrgang 1994, Seite 413 ff.).
  - i) Veröffentlichung von persönlichen Daten (z. B. Alterjubiläum) in Pfarrbriefen und ähnlichen Publikationen vom 08.01.1998 (veröffentlicht im Kirchlichen Anzeiger für das Bistum Hildesheim, Jahrgang 1998, Seite 24 ff.).
2. Die oben genannten bereichsspezifischen datenschutzrechtlichen Regelungen gelten auch weiterhin.

Hildesheim, den 18.12.2003

Bernert  
Generalvikar

# **Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Hildesheim**

## **Inhaltsübersicht**

- § 1 Datenkatalog
- § 2 Technische und organisatorische Maßnahmen
- § 3 Datenübermittlung an andere Schulen und sonstige Stellen
- § 4 Datenübermittlung an Beratungsdienste und an den schulärztlichen Dienst
- § 5 Klassenbücher
- § 6 Weitergabe von Schülerdaten, Elterndaten und Lehrerdaten
- § 7 Inkrafttreten

Gemäß § 20 Abs. 1 der Anordnung über den kirchlichen Datenschutz - KDO - wird zur Regelung des Schutzes personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Hildesheim folgende Anordnung erlassen:

Die katholischen Schulen in freier Trägerschaft in der in der Diözese Hildesheim sind für die Erfüllung ihrer Aufgaben darauf angewiesen, Daten von Mitarbeitern, Erziehungsberechtigten, Schülern und Ausbildungsbetrieben zu erheben und weiterzuverarbeiten. Dem entspricht ihre Pflicht, die Daten vertraulich zu behandeln, sie nur zu verwenden, soweit es für die rechtmäßige Erfüllung ihrer Aufgaben erforderlich ist, und die Betroffenen vor jedem Missbrauch zu schützen.

Was zur Aufgabenerfüllung notwendig ist, ergibt sich aus der in der Grundordnung für die katholischen Schulen in freier Trägerschaft in der Diözese Hildesheim vom 1. April 1985 genannten Zielsetzung.

## **§ 1 Datenkatalog**

- (1) Folgende Daten von Schülern dürfen gespeichert werden
  - Ordnungsbegriff, Schülernummer
  - Name, Vorname
  - Anschrift
  - Telefonnummer
  - Geburtsdatum
  - Geburtsort
  - Familienstand
  - Staatsangehörigkeit
  - Konfession
  - Taufdatum
  - Geschlecht
  - Krankenversicherung
  - Wohnsitzpfarrei
  - Schulversäumnisse
  - Beurlaubung vom Schulbesuch
  - Daten zum schulischen Werdegang
  - Entlassungsart

Funktionen in der Schule  
Leistungsdaten  
sonstige Qualifikationsnachweise  
Kurswahl  
Versetzungsentscheidungen  
Schulgeldpflicht / Schulgeldhöhe  
Bankverbindung des Zahlenden  
Teilnahme am Schülertransport  
Fahrtkostenerstattungen (Betrag und Zeitraum)  
und / oder Lehrmittelkostenerstattungen  
Bankverbindungen des Empfängers  
Klasse, Klassenlehrer, Tutor  
beim Besuch berufsbildender Schulen Name und Anschrift des jeweiligen Ausbildungsbetriebes, der Praktikantenstelle oder der sie ersetzenden Institution  
Ausbildungsberuf, Beginn und Ende der betrieblichen Ausbildung  
Berufsschultag

- (2) Folgende Daten von Erziehungsberechtigten dürfen gespeichert werden:  
Name, Vorname, Anschrift der Erziehungsberechtigten  
Telefonnummer  
Staatsangehörigkeit  
Konfession  
Funktionen in der Schule
- (3) Weitere Daten wie Verhaltensdaten, Daten von Geschwistern, Daten zu gesundheitlichen Auffälligkeiten (Behinderungen), Daten zu pädagogischen, sozialen und therapeutischen Maßnahmen und deren Ergebnisse dürfen grundsätzlich nur mit Einwilligung der Betroffenen bzw. eines Erziehungsberechtigten gespeichert werden.  
Die Einwilligung ist zu ersetzen, wenn
- a) die Betroffenen sich trotz eingehender Bemühung durch die Schule nicht geäußert haben oder
  - b) die Betroffenen trotz eingehender Beratung durch die Schule die Einwilligung versagt haben und die Speicherung im Interesse des Schülers oder für die pädagogische Arbeit einer Schule zwingend notwendig ist.

## § 2 Technische und organisatorische Maßnahmen

- (1) Die in den Schulen gespeicherten personenbezogenen Daten dürfen nur denen zugänglich gemacht werden, die die Daten zur Erfüllung ihres dienstlichen Auftrages benötigen. Sie sind vor Unbefugten zu sichern und in abschließbaren Schränken aufzubewahren. Zugangsberechtigt sind außer der Schulsekretärin und dem Schulleiter bzw. Schulträger nur die jeweils für den Schüler zuständigen Lehrer.
- (2) Für die in den Schulen vorhandenen EDV-Anlagen sollte eine schriftliche Benutzerordnung erlassen werden. In der Benutzerordnung sind die näheren Modalitäten im Umgang mit der EDV-Anlage, die Fragen der Zugriffsberechtigung und die Verantwortlichkeit für die EDV-Anlage, die Weitergabe von Daten an Dritte sowie die Vernichtung eventuell vorhandener Ausdrücke zu regeln. Die Datenverarbeitung der Schulverwaltung ist von der Datenverarbeitung für den Unterrichtsbereich zu trennen.

### **§ 3 Datenübermittlung an andere Schulen und sonstige Stellen**

- (1) Beim Wechsel eines Schülers in eine andere Schule können Anschriften und Geburtsdaten, Daten zur Staatsangehörigkeit, zur Konfession, zur Einschulung, zu Versetzungen, zum Vorrücken und Wiederholen von Jahrgangsstufen, die beiden letzten Zeugnisbögen sowie - nur mit Genehmigung der Betroffenen - Daten über Erkrankungen und Behinderungen übermittelt werden. Besteht im Einzelfall ein begründetes Interesse an weiteren von der abgehenden Schule gespeicherten Daten, können sie der aufnehmenden Schule übermittelt werden. Beim Übergang in die gymnasiale Oberstufe dürfen auch Daten über den Unterricht in den Fremdsprachen sowie Daten über den Unterricht, der vor Beginn der Klasse 12 abgeschlossen wurde, übermittelt werden.
- (2) Eine aufnehmende (abgebende) Schule kann im Einzelfall der bisherigen Schule Daten über die Lernentwicklung und Verhaltensentwicklung übermitteln, wenn dies der pädagogischen Arbeit dieser Schule dient.
- (3) An sonstige Stellen (z.B. Praktikantenstellen) können Daten übermittelt werden, sofern dies zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich ist. Wegen der Voraussetzungen wird auf die §§ 10 und 11 KDO verwiesen.

### **§ 4 Datenübermittlung an Beratungsdienste und an den schulärztlichen Dienst**

- (1) An Beratungsdienste und an den schulärztlichen Dienst dürfen gespeicherte Daten, soweit es erforderlich ist, übermittelt werden, wenn entsprechende Beratungen oder Untersuchungen zum Wohle der Schüler angestrebt werden. Die Übermittlung ist zulässig, wenn die Erziehungsberechtigten oder der volljährige Schüler zustimmen. Bei Einzelberatung oder Einzeluntersuchung bedarf es der schriftlichen Zustimmung mindestens eines Erziehungsberechtigten oder des volljährigen Schülers,
- (2) Sich aus Beratungen und Untersuchungen ergebende Gutachten oder Befunde unterliegen strengster Vertraulichkeit. Auskünfte daraus dürfen nur den Erziehungsberechtigten, dem volljährigen Schüler und dem vormaligen Erziehungsberechtigten von dem jeweiligen Beratenen erteilt werden. Die Schulen erhalten Auskünfte, sofern sie zur Erfüllung des Auftrags der Schule notwendig sind. Ärztliche Gutachten und Sachverhalte, die einzelnen Lehrern oder dem Schulleiter von Erziehungsberechtigten oder Schülern zu ihrer persönlichen Information anvertraut worden sind, dürfen nur mit dem Einverständnis der Betroffenen an eine andere Stelle weitergegeben werden.

### **§ 5 Klassenbücher**

- (1) In Klassenbücher dürfen folgende personenbezogene Informationen über Schüler und Erziehungsberechtigte eingetragen werden:  
Name, Geburtsdatum und Konfession des Schülers,  
besondere Funktionen in der Schule, Hinweise auf die Teilnahme oder Nichtteilnahme an bestimmten Schulveranstaltungen, Fehlzeiten,  
beim Besuch berufsbildender Schulen: die Ausbildungsberufe der Schüler sowie die ausbildenden Firmen nebst Anschriften und Telefonnummern,  
Funktionen der Erziehungsberechtigten in der Schule,

Namen, Anschriften und Telefonnummern, unter denen die Erziehungsberechtigten oder andere Angehörige erreichbar sind. Die Erziehungsberechtigten können verlangen, dass diese Eintragungen in das Klassenbuch unterbleiben. Auf die sich daraus möglicherweise ergebenden Nachteile sind die Erziehungsberechtigten hinzuweisen.

- (2) Mit schriftlicher Zustimmung zumindest eines Erziehungsberechtigten können in Einzelfällen auch Erkrankungen von Schülern und die in Notfällen zu ergreifenden Maßnahmen im Klassenbuch vermerkt werden.
- (3) Alle anderen erforderlichen personenbezogenen Daten über Schüler und Erziehungsberechtigte dürfen nur in gesonderten Büchern, Listen, Akten oder Dateien gespeichert werden. Dies gilt auch für Leistungsdaten wie Noten der Klassenarbeiten und Zensurenlisten sowie für die Eintragung eines mündlichen Tadel.
- (4) Geeignete Schüler, die sich freiwillig dazu bereit erklären, können die Lehrkräfte während der täglichen Unterrichtszeit bei Transport, Aufbewahrung und Führung der Klassenbücher unterstützen. Die Notwendigkeit, das Klassenbuch in Rahmen der gegebenen Möglichkeiten gegen unbefugte Einsicht zu sichern, ist mit diesen Schülern in altersgemäßer Weise zu besprechen.
- (5) Klassenbücher dürfen nur in verschlossenen bzw. durch Zugangsberechtigte beaufsichtigten Räumen aufbewahrt werden.

## **§ 6 Weitergabe von Schülerdaten, Elterndaten und Lehrerdaten**

- (1) Die Weitergabe von Schülerdaten, Elterndaten und Lehrerdaten zu Werbezwecken jeder Art und die Übermittlung der Namen und Vornamen von Schulanfängern oder Schulabgängern an die Presse ist nicht zulässig, es sei denn die Betroffenen haben der Übermittlung schriftlich zugestimmt,
- (2) Die Weitergabe von Adressdaten von Schülern an die zuständigen örtlichen Kirchengemeinden ist zulässig.
- (3) Listen mit Namen, Vornamen, Anschriften und Telefonnummern der Schüler einer Klasse können zur Erleichterung des Kontaktes der Schüler und Erziehungsberechtigten untereinander an alle Erziehungsberechtigten und Schüler der Klasse verteilt werden, wenn diese vorher in geeigneter Form Gelegenheit hatten, zu widersprechen.
- (4) Zur Vorbereitung eines Klassentreffens kann die Schule ehemaligen Schülern die Anschriften von früheren Mitschülern überlassen, sofern sie darauf hingewiesen hat, dass die Adressen nur zum angegebenen Zweck verwendet werden dürfen.
- (5) Die schulinterne Übermittlung von Namen, Anschriften und Telefonnummern der Mitglieder schulischer Gremien ist zulässig.
- (6) Bei volljährigen Schülern darf die Schule in Wahrnehmung ihrer pädagogischen Verantwortung ohne deren Einverständnis den vormals Erziehungsberechtigten Auskunft erteilen.
- (7) Die Weitergabe von Daten aus Lehrerverzeichnissen ist zulässig, wenn dies zur rechtmäßigen Erfüllung der Aufgaben der weitergebenden Stelle oder des Empfängers erforderlich ist.

## **§ 7 Inkrafttreten**

Diese Anordnung tritt am 01. Januar 1994 in Kraft.

# **Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Hildesheim**

Gemäß § 20 Abs. 1 der Anordnung über den Kirchlichen Datenschutz- KDO - wird zur Regelung des Schutzes personenbezogener Daten in katholischen Krankenhäusern in der Diözese Hildesheim folgende Ordnung erlassen:

## **§ 1 Geltungsbereich**

- (1) Diese Ordnung gilt für alle katholischen Krankenhäuser in der Diözese Hildesheim ohne Rücksicht auf deren Rechtsform oder die Trägerschaft des jeweiligen Krankenhauses.
- (2) Diese Ordnung regelt den Schutz personenbezogener Daten von Patienten eines Krankenhauses (Patientendaten), unabhängig von der Form ihrer Erhebung, der Art ihrer Verarbeitung und Nutzung. Als Patientendaten gelten auch personenbezogene Daten Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden.
- (3) Soweit in dieser Ordnung nichts anderes bestimmt ist, gelten die Anordnung über den Kirchlichen Datenschutz und die zu ihrer Durchführung ergangenen Vorschriften. Weitergehende Rechtsvorschriften, insbesondere die der ärztlichen Schweigepflicht, bleiben unberührt.

## **§ 2 Umfang der Datenverarbeitung**

- (1) Patientendaten dürfen nach Maßgabe der §§ 7 und 9 der Anordnung über den Kirchlichen Datenschutz im Krankenhaus nur erhoben, verarbeitet und genutzt werden, soweit
  1. dies im Rahmen des Behandlungsverhältnisses einschließlich der verwaltungsmäßigen Abwicklung und Leistungsberechnung, zur Erfüllung der mit der Behandlung in Zusammenhang stehenden Dokumentationspflichten oder eines damit zusammenhängenden Rechtsstreites erforderlich ist,
  2. eine staatliche oder kirchliche Rechtsvorschrift dies vorschreibt oder erlaubt oder
  3. der Betroffene eingewilligt hat.
- (2) Die Einwilligung gemäß Abs. 1 Nr. 3 bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Wird die Einwilligung wegen besonderer Umstände nur mündlich erteilt, so ist dies vom Krankenhaus schriftlich in den Unterlagen zu vermerken. Wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist der Betroffene hierauf schriftlich hinzuweisen.
- (3) Die Angabe der Religionszugehörigkeit bei der Patientenaufnahme ist freiwillig.

## **§ 3 Übermittlung und Nutzung von Patientendaten im Krankenhaus**

- (1) Die Übermittlung und Nutzung von Patientendaten innerhalb des Krankenhauses einschließlich der Krankenhauseesorge und des Sozialdienstes im Krankenhaus sind nur zulässig, soweit dies zur jeweiligen Aufgabenerfüllung erforderlich ist.
- (2) Für die Übermittlung von Patientendaten zwischen Behandlungseinrichtungen verschiedener Fachrichtungen in einem Krankenhaus (Fachabteilungen) gelten die §§ 4 und 7 Abs. 2 entsprechend.

- (3) Für die Qualitätssicherung der Krankenversorgung sowie die Aus-, Fort- und Weiterbildung ist die Nutzung von Patientendaten nur insoweit zulässig, als diese Zwecke nicht mit anonymisierten Daten erreicht werden können.

#### **§ 4 Übermittlung von Patientendaten an Personen und Stellen außerhalb des Krankenhauses und deren Nutzung**

- (1) Die Übermittlung von Patientendaten an Personen oder Stellen außerhalb des Krankenhauses und deren Nutzung ist neben der Erfüllung von Pflichten aufgrund bestehender Rechtsvorschriften nur zulässig, soweit sie erforderlich sind zur
  1. Behandlung einschließlich der Mit-, Weiter- und Nachbehandlung, wenn nicht der Patient nach Hinweis auf die beabsichtigte Übermittlung etwas anderes bestimmt hat,
  2. Abwehr einer gegenwärtigen Gefahr für das Leben, die Gesundheit oder die persönliche Freiheit des Patienten oder eines Dritten, sofern diese Rechtsgüter das Geheimhaltungsinteresse des Patienten erheblich überwiegen und die Abwendung der Gefahr ohne die Übermittlung nicht möglich ist,
  3. Durchführung qualitätssichernder Maßnahmen in der Krankenhausversorgung, wenn bei der beabsichtigten Maßnahme das Interesse der Allgemeinheit an der Durchführung die schutzwürdigen Belange des Patienten erheblich überwiegt,
  4. Abrechnung und Durchsetzung von Ansprüchen aufgrund der Behandlung,
  5. Unterrichtung des Seelsorgers der für den Patienten zuständigen Gemeinde, sofern der Patient der Übermittlung nicht widersprochen hat oder Anhaltspunkte dafür bestehen, dass eine Übermittlung nicht angebracht ist. Der Patient ist bei der Aufnahme ausdrücklich darauf hinzuweisen, dass er der Übermittlung widersprechen kann.
  6. Unterrichtung von Angehörigen, soweit es zur Wahrung ihrer berechtigten Interessen erforderlich ist, schutzwürdige Belange des Patienten nicht beeinträchtigt werden und die Einholung der Einwilligung für den Patienten gesundheitlich nachteilig wäre.

Im Übrigen ist eine Übermittlung nur mit Einwilligung des Patienten zulässig. Die Übermittlung medizinischer Patientendaten darf nur durch den Arzt erfolgen.
- (2) Personen oder Stellen, an die Patientendaten weitergegeben worden sind, dürfen diese zu dem Zweck verwenden, zu dem sie ihnen übermittelt wurden. Im Übrigen haben sie diese Daten unbeschadet sonstiger Datenschutzbestimmungen in demselben Umfang geheimzuhalten wie das Krankenhaus selbst.

#### **§ 5 Löschung und Sperrung von Daten**

- (1) Patientendaten sind unverzüglich zu löschen, wenn sie zur Erfüllung der Aufgaben, für die sie erhoben wurden, nicht mehr erforderlich sind, die vorgeschriebenen Aufbewahrungsfristen abgelaufen sind und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Gespeichert bleiben darf ein Datensatz, der für das Auffinden der Behandlungsdokumentation erforderlich ist.
- (2) Bei Daten, die im automatisierten Verfahren mit der Möglichkeit des Direktabrufes gespeichert sind, ist die Möglichkeit des Direktabrufes zu sperren, sobald die Behandlung

des Patienten im Krankenhaus abgeschlossen ist, die damit zusammenhängenden Zahlungsvorgänge abgewickelt sind und das Krankenhaus den Bericht über die Behandlung erstellt hat, spätestens jedoch ein Jahr nach Abschluß der Behandlung des Patienten.

## **§ 6 Datenverarbeitung im Auftrag**

Das Krankenhaus darf sich zur Verarbeitung von Patientendaten anderer Personen und Stellen nur dann bedienen, wenn die Einhaltung der geltenden Datenschutzbestimmungen und der Geheimhaltungspflichten nach § 203 StGB gewährleistet ist.

## **§ 7 Patientendaten und Forschung**

- (1) Patientendaten, die innerhalb einer Fachabteilung des Krankenhauses gespeichert sind, dürfen für eigene wissenschaftliche Forschungsvorhaben nur von den dort beschäftigten Personen, die der ärztlichen Schweigepflicht unterliegen, verarbeitet oder genutzt werden.
- (2) Patientendaten dürfen zum Zweck einer bestimmten wissenschaftlichen Forschung nur dann an Dritte übermittelt, durch diese verarbeitet oder genutzt werden, wenn der Zweck dieses Forschungsvorhabens nicht auf andere Weise erfüllt werden kann und
  1. das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegt oder
  2. es nicht zumutbar ist, die Einwilligung einzuholen, und schutzwürdige Belange des Patienten nicht beeinträchtigt werden.

In allen anderen Fällen ist die Übermittlung von Patientendaten an Dritte und deren Verarbeitung oder Nutzung durch sie nur zulässig, soweit der Patient eingewilligt hat.

- (3) Sobald es der Forschungszweck gestattet, sind die personenbezogenen Daten zu anonymisieren. Merkmale, mit deren Hilfe ein Personenbezug wiederhergestellt werden kann, sind gesondert zu speichern; sie sind zu löschen, sobald der Forschungszweck es erlaubt.
- (4) Veröffentlichungen von Forschungsergebnissen dürfen keinen Rückschluss auf die Person zulassen, deren Daten verarbeitet oder genutzt werden.
- (5) Soweit die Bestimmungen dieser Ordnung auf den Empfänger keine Anwendung finden, dürfen Patientendaten nur übermittelt werden, wenn sich dieser verpflichtet,
  1. die Daten nur für das von ihm genannte Forschungsvorhaben zu verwenden.
  2. die Bestimmungen der Absätze 3 und 4 einzuhalten und
  3. die Vorschriften der §§ 4, 6 und 8 dieser Ordnung zu beachten und
  4. den Beauftragten für den Datenschutz auf Verlangen Einsicht und Auskunft zu gewähren.

Der Empfänger muss nachweisen, daß bei ihm die technischen und organisatorischen Voraussetzungen zur Erfüllung seiner Verpflichtung nach Nummer 2 vorliegen.

## **§ 8 Schutzmaßnahmen**

- (1) Durch technische und organisatorische Maßnahmen, die erforderlich und angemessen sind, ist der Schutz der Patientendaten zu gewährleisten.
- (2) Jeder Krankenhausträger bestellt einen oder mehrere Betriebsbeauftragte für den Datenschutz; es kann auch ein gemeinsamer Betriebsbeauftragter für mehrere Krankenhäuser

bestellt werden. Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt wird und die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.

## **§ 9 Aufzeichnung und Auskunftserteilung**

- (1) In allen Fällen des § 4 Abs. 1 hat die übermittelnde Stelle den Empfänger, die Art der übermittelten Daten und die betroffenen Patienten aufzuzeichnen. Gleiches gilt für die Fälle des § 7 Abs. 2 mit der Maßgabe, dass auch das vom Empfänger genannte Forschungsvorhaben aufzuzeichnen ist.
- (2) Dem Patienten ist auf Verlangen unentgeltlich
  1. Auskunft über die zu seiner Person gespeicherten Daten sowie über die Personen und Stellen zu erteilen, an die personenbezogene Daten weitergegeben wurden und
  2. Einsicht in seine Behandlungsdokumentation zu gewähren.
- (3) Das Krankenhaus soll die gemäß Abs. 2 zu gewährende Auskunft über die den Patienten betreffenden medizinischen Daten und die Einsicht in seine Behandlungsdokumentation nur durch einen Arzt vermitteln lassen.
- (4) Ein Anspruch auf Auskunft oder Einsichtnahme steht dem Patienten nicht zu, soweit berechtigte Geheimhaltungsinteressen Dritter, deren Daten zusammen mit denen des Patienten aufgezeichnet sind, überwiegen.

## **§ 10 Inkrafttreten**

Diese Ordnung tritt am 01. Januar 1994 in Kraft.

## - Telefax -

### **Datenschutz bei der Übermittlung personenbezogener Daten über Telefaxgeräte**

Die Vorteile des Telefaxdienstes und die Tatsache, dass beliebige Vorlagen schnell übertragen und beim Empfänger *sofort*<sup>1</sup> originalgetreu - und offen! - ausgedruckt werden, lassen bei Dokumenten mit personenbezogenem Inhalt Probleme entstehen.

#### **Fernmeldegeheimnis**

Nach den Vorschriften des Fernmeldeanlagengesetzes ist „jeder, der eine für den öffentlichen Verkehr bestimmte Fernmeldeanlage betreibt, beaufsichtigt oder bedient oder sonst bei ihrem Betrieb tätig ist, zur Wahrung des Fernmeldegeheimnisses verpflichtet“. Dies gilt auch z.B. für Mitarbeiterinnen/Mitarbeiter, die ein eingegangenes Telefax dem Gerät entnehmen, um es dem Empfänger zuzuleiten oder die die Sende-/Empfangsprotokolle ausdrucken lassen und verwalten. Die Mitarbeiterinnen/Mitarbeiter sollten auf die Bedeutung des Fernmeldegeheimnisses, insbesondere die Folgen eines Verstoßes hingewiesen werden.

#### **Sende-/Empfangsprotokolle**

Telefaxgeräte erzeugen automatisch und/oder auf Wunsch Sende-/Empfangsprotokolle, die bezüglich jedes Vorganges u. a. den Zeitpunkt der Sendung bzw. des Empfangs und die Anschlusskennung der anderen Station enthalten. Diese Daten unterliegen dem besonderen Schutz des Fernmeldegeheimnisses. Die Protokolle müssen daher entsprechend sorgfältig behandelt werden.

#### **Kenntnisnahme durch Unbefugte**

Weil Telefaxsendungen (z. B. vertrauliche Dokumente) beim erreichten Empfänger offen ankommen, ist bei der Versendung besondere Sorgfalt geboten. Vor der Absendung muss die Gültigkeit der bekannten Anschlussnummer gewährleistet sein.

#### **Anschlusskennung des Empfängers**

Durch Falschwahl sowohl beim Absender als auch im Übertragungsnetz der Deutschen Bundespost kann es dazu kommen, daß ein anderer als der gewünschte Anschluss erreicht wird. Zudem kann sich, da frei gewordene Anschlussnummern durch die Post sofort wieder neu vergeben werden, hinter einer bekannten und auch richtig angewählten Anschlussnummer unerwartet ein anderer Partner verbergen. Bei jeder Sendung ist deshalb zu überprüfen, ob auch tatsächlich der richtige Anschluss/Partner erreicht wird.

#### **Zeitversetzte Sendungen**

Bei Sendungen ins Ausland ist die Ortszeit zu überprüfen. Es ist je nach Art des Inhalts sicherzustellen, dass ein Telefax dort nicht außerhalb der Dienstzeit ankommt und somit durch Unbefug-

---

<sup>1</sup> Zusatz „sofort“ nur in der im Bistum Hildesheim verkündeten Fassung

te Einsicht genommen werden könnte. Dieser Gesichtspunkt ist auch im Inland dann zu beachten, wenn ein Telefax nicht sofort abgesandt, sondern von der Möglichkeit der zeitversetzten Sendung Gebrauch gemacht wird.

### **Anrufumleitung, -weiterrichtung**

Für Telefaxgeräte, die in Kommunikationsanlagen (Telefonanlagen) eingesetzt sind, kann - soweit vorhanden - die Möglichkeit der Anrufumleitung und -weiterrichtung genutzt werden. Dies kann dazu führen, dass eine Sendung bei einem (anderen als dem angewählten) Empfangsgerät ankommt, das in einem fachlich unzuständigen Bereich aufgestellt ist. Dadurch könnte es zu einer datenschutzrechtlich unzulässigen Übermittlung kommen. Dieses Risiko kann nur durch Überprüfung der rückgesendeten Kennung ausgeschlossen werden.

### **Besonders schutzbedürftige Daten**

*Insbesondere personenbezogene Daten genießen einen erhöhten Persönlichkeitsschutz<sup>1</sup>*

Bei der **Übermittlung personenbezogener Daten**, insbesondere solcher, die sich auf

- strafbare Handlungen
- Ordnungswidrigkeiten
- religiöse oder politische Anschauungen sowie
- bei der Übermittlung durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse
- gesundheitliche Verhältnisse
- Auffälligkeiten

beziehen, sollte Vorsorge getroffen werden, um die Rechte der Betroffenen zu wahren. *Solche Daten sind grundsätzlich per Brief mitzuteilen<sup>1</sup>*. Sie sind nur dann per Telefax zu übermitteln, wenn dies von der **Eilbedürftigkeit** her geboten und durch besondere Vorkehrungen sichergestellt ist, dass die Sendung nur dem richtigen Empfänger zugeht. Neben der Beachtung dieser Hinweise ist es geboten, unmittelbar vor der Sendung eine telefonische Vereinbarung möglichst auch über persönliche Entgegennahme der Sendung zu treffen.

### **Dokumentation, Vollständigkeit**

Jeder Sendung sollte ein „Vorblatt“ begefügt werden, welches Absender, dessen Telefax- und Telefonnummer (für Rückrufe) sowie die Gesamtzahl der gesendeten Seiten ausweist.

Es sollte möglichst für jede Sendung ein Sendeprotokoll erzeugt und dem Vorgang begefügt werden. Durch Namenskürzel und Tagesdatum auf den Originalen sollte die Überprüfung und Richtigkeit der gesendeten Telefaxe sichergestellt werden.

Für ankommende Telefaxe gilt das gleiche, um die Einsichtnahme und die Weitergabe zu dokumentieren.

Da das Schreibbild eines Telefaxes oftmals nach kurzer Zeit bis zur Unkenntlichkeit verblasst, ist es angebracht, nach Eingang eines Telefaxes eine Kopie als Zweitschrift zu erstellen.

---

<sup>1</sup> Zusatz, der im Bistum Hildesheim verkündeten Fassung

## **Räumliche Unterbringung**

Telefaxgeräte sollten in solchen Räumen untergebracht werden, in denen gewährleistet ist, dass Telefaxsendungen nicht unbeobachtet ankommen und von Unbefugten entnommen oder eingesehen werden können.

## **Organisatorische Regelungen**

Die Telefaxgeräte bzw. Telefaxanlage sollten nur nach An- bzw. Einweisung genutzt werden. Dabei sollten insbesondere die grundsätzlichen Sicherungsvorkehrungen sowie die Verantwortlichkeit festgelegt werden.

Osnabrück, 14. November 1991

Das Bischöfliche Generalvikariat

Hildesheim, den 01. November 1992

Schenk  
Generalvikar

## **Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft in der Diözese Hildesheim**

Gemäß § 20 Abs. 1 der Anordnung über den kirchlichen Datenschutz - KDO - wird zur Regelung des Schutzes personenbezogener Daten bei Friedhöfen in kirchlicher Trägerschaft in der Diözese Hildesheim folgende Ordnung erlassen.

### **§ 1 Datenverarbeitung**

- (1) Zur Bewirtschaftung und Verwaltung der Friedhöfe, insbesondere zur Festsetzung und Einziehung von Gebühren, dürfen vom Friedhofsträger oder in seinem Auftrag folgende personenbezogene Daten der Verstorbenen verarbeitet werden:
  1. Vor-, Geburts- und Nachname,
  2. letzte Adresse,
  3. Geburts- und Sterbedatum,
  4. Sterberegisternummer,
  5. Ort und Zeitpunkt der Einäscherung,
  6. Einäscherungsnummer,
  7. Zeitpunkt der Bestattung,
  8. Bestattungsnummer,
  9. Art, Lage und Zustand der Grabstelle,
  10. Bestattungen in der Grabstelle,
  11. Dauer des Nutzungsrechts,
  12. Ruhefrist,
  13. Vorhandensein von Grabmalen und Einfassungen sowie Datum der Genehmigung,
  14. Name und Adresse des Bestatters,
  15. Leistungen des Friedhofsträgers,
  16. Konfession und Gemeindezugehörigkeit des Verstorbenen.
- (2) Zu den in Absatz 1 genannten Zwecken dürfen vom Friedhofsträger oder in seinem Auftrag folgende personenbezogene Daten der Nutzungsberechtigten verarbeitet werden:
  1. Vor-, Geburts- und Nachnamen sowie Konfession,
  2. Adresse,
  3. Geburtsdatum,
  4. Art, Lage und Zustand der Grabstelle,
  5. Namen und Adressen von Bevollmächtigten,
  6. Namen, Adresse und Geburtsdatum des vom Nutzungsberechtigten benannten Nachfolgers im Nutzungsrecht.
- (3) Zur Klärung der Nutzungsrechtsnachfolge dürfen vom Friedhofsträger oder in seinem Auftrag folgende personenbezogene Daten der Angehörigen der Verstorbenen oder der Nutzungsberechtigten verarbeitet werden:
  1. Vor-, Geburts- und Nachnamen,
  2. Adresse,
  3. Geburtsdatum,
  4. Verhältnis zum letzten Nutzungsberechtigten,
  5. Sterbedatum des letzten Nutzungsberechtigten,

6. Art, Lage und Zustand der Grabstelle,
  7. Namen und Adressen von Bevollmächtigten.
- (4) Im Rahmen der Zulassung und Überwachung der auf den Friedhöfen tätigen Gewerbetreibenden des Friedhofs- und Bestattungsgewerbes dürfen vom Friedhofsträger oder in seinem Auftrag folgende personenbezogene Daten verarbeitet werden:
1. Vor- und Nachnamen,
  2. Adresse,
  3. Art des Gewerbes,
  4. Zulassung,
  5. Tätigkeitsbeschränkungen oder -verbote.
- (5) Die Verarbeitung der personenbezogenen Daten nach den Absätzen 1, 2, 3 und 4 darf auch im automatisierten Verfahren erfolgen.
- (6) Die in den Absätzen 1 bis 4 genannten Daten sind zu löschen, wenn sie nicht mehr benötigt werden.

Die in Absatz 1 genannten Daten der Verstorbenen müssen für den Zeitraum der Ruhefrist aufbewahrt werden, solange ein Nutzungsrecht an der Grabstelle besteht, das sich auf diese Verstorbenen bezieht. Nach Ablauf der in Satz 2 genannten Fristen dürfen die Daten der Verstorbenen nur noch gesondert, durch technische und organisatorische Maßnahmen gesichert, aufbewahrt werden. Sie dürfen dann nur noch verarbeitet oder genutzt werden, wenn Angehörige um Auskunft nachsuchen oder dies für wissenschaftliche Zwecke erforderlich ist. Die in den Absätzen 2 und 3 genannten Daten sind von einer Umschreibung des Nutzungsrechts an bis zur folgenden Umschreibung, mindestens jedoch 10 Jahre, aufzubewahren.

## **§ 2 Datenübermittlung**

- (1) Wird die Bestattung von einer anderen Kirchengemeinde als der zuständigen Kirchengemeinde oder einem sonstigen kirchlichen Bestattungsberechtigten vorgenommen, dürfen vom Friedhofsträger oder in seinem Auftrag zum Zwecke der Bestattung folgende Daten der Verstorbenen an die andere Kirchengemeinde oder den sonstigen kirchlichen Bestattungsberechtigten übermittelt werden:
1. Vor-, Geburts- und Nachnamen,
  2. Geburts- und Sterbedatum,
  3. letzte Adresse,
  4. Sterberegisternummer,
  5. Ort und Zeitpunkt der Einäscherung,
  6. Einäscherungsnummer,
  7. Ort und Zeitpunkt der Bestattung,
  8. Konfession und Gemeindezugehörigkeit des Verstorbenen.
- (2) Bei Umbettungen von Leichen dürfen der zuständigen Gesundheitsbehörde folgende Daten des Verstorbenen übermittelt werden:
1. Vor-, Geburts- und Nachnamen,
  2. Geburts- und Sterbedatum.
- (3) Lässt sich ein Friedhofsträger bei der Genehmigung von Grabmalen bezüglich deren Gestaltung von Sachverständigen beraten, so dürfen den Sachverständigen zur Prüfung der vorgelegten Entwürfe folgende Daten übermittelt werden:

1. Name des Verstorbenen,
  2. Geburts- und Sterbedatum des Verstorbenen,
  3. Name und Anschrift des Entwurfsverfassers.
- (4) Zum Zweck der Vollstreckung von Friedhofsgebühren dürfen der zuständigen Behörde folgende Daten übermittelt werden:
1. Name, Vorname und Anschrift des Gebührenschuldners,
  2. Höhe der Forderung,
  3. Name, Vorname und letzte Anschrift der/des Verstorbenen,
  4. Datum der Bestattung,
  5. Datum des Gebührenbescheides und der Mahnung,
  6. Datum und Betrag eventueller Teilzahlungen.
- (5) Die Lage einer Grabstelle darf Dritten auf entsprechende Nachfrage bekanntgegeben werden, wenn diese ein berechtigtes Interesse glaubhaft machen und anzunehmen ist, dass schutzwürdige Belange des Verstorbenen nicht beeinträchtigt werden.

### **§ 3 Inkrafttreten**

Diese Ordnung tritt am 1. Januar 1993 in Kraft.

## **Schutz von Computerprogrammen**

Besonderer Schutz von Computerprogrammen nach dem Urheberrechtsgesetz<sup>1</sup>

Aufgrund einer Gesetzesänderung sind seit dem 09.06.1993 Computerprogramme unter den besonderen Schutz des Urheberrechtsgesetzes gestellt. Danach sind insbesondere die Vervielfältigung von Computerprogrammen und die Weitergabe von Programm-Kopien verboten. Gesetzesverstöße können mit Freiheitsstrafe bis zu 3 Jahren oder mit Geldstrafe geahndet werden.

Daher erscheint es notwendig, für den dienstlichen Einsatz von PC auf die folgenden Punkte aufmerksam zu machen:

1. Die Verantwortung für den PC liegt bei dem Mitarbeiter, der - überwiegend - mit dem PC arbeitet. Er trägt dafür Sorge, daß kein unberechtigter Zugriff auf den PC - insbesondere auf die darin enthaltenen Daten und Programme - erfolgt. Dieses gilt vor allem beim - auch nur kurzfristigen - Verlassen des Arbeitsplatzes. Ein Schutz kann z.B. dadurch erreicht werden, dass der PC die Software, die Datenträger und die Handbücher unter Verschluss gehalten werden. In speziellen Fällen wird empfohlen, entsprechende Sicherheitsprogramme (z.B. PC-Guard) zum Schutz des Systems, der Programme und der Daten einzusetzen.
2. Auf dem PC dürfen nur Originalprogramme eingesetzt werden. Erforderlich und erlaubt ist lediglich das Erstellen einer Sicherungskopie des Programms. Verboten ist dagegen das Kopieren von Programmen zur Weitergabe sowohl an Kollegen als auch an außenstehende Personen. Außer der Sicherungskopie dürfen keine weiteren Programmkopien erstellt oder verwendet werden.
3. Soweit Zweifel bestehen, ob es sich bei dem verwendeten Programm um ein ordnungsgemäßes registriertes Originalprogramm handelt, können Sie sich an den EDV-Beauftragten wenden.
4. Grundsätzlich dürfen auch keine Public-Domain- und Shareware-Programme eingesetzt werden. Soweit dies doch geschehen soll, müssen diese beim Programmhersteller ordnungsgemäß registriert werden. Hierbei ist zu bedenken, dass über den Einsatz solcher Programme leicht Viren übertragen werden. Ein solcher Einsatz sollte immer mit dem EDV-Beauftragten (siehe unten) abgestimmt werden.
5. Auf dem PC dürfen nur dienstlich genutzte Programme eingesetzt werden.
6. Es ist eine Bestandsaufnahme erforderlich. Hierbei sollen alle derzeit schon vorhandenen und genutzten Hard- und Soft-Ware-Systeme registriert werden. Hierzu bitten wir um Mitteilung über verwendete Hard- und Soft-Ware an den EDV-Beauftragten, soweit dieses nicht schon geschehen ist. Ebenso bitten wir zukünftig um Meldung der jeweils neu geschaffenen PC-Programme.
7. Die für den Einsatz von Informationstechnik bereits geltenden Regelungen, insbesondere die gesetzlichen Vorschriften des Datenschutzes sind zu beachten.

Für alle Rückfragen steht Ihnen der EDV-Beauftragte für das Bistum Hildesheim, Herr de Lorenzo, Bischöfliches Generalvikariat, Domhof 18-21, Hildesheim, Telefon 307-425, zur Verfügung.

Hildesheim, den 1. Oktober 1993

Bischöfliches Generalvikariat

---

<sup>1</sup> verkündet im Kirchlichen Anzeiger für das Bistum Hildesheim, Jahrgang 1994, Seite 49 f.

## - Informationstechnik -

### **Richtlinie zum Einsatz von Arbeitsplatzcomputern in der Diözese Hildesheim<sup>1</sup>, (in der Diözese Osnabrück<sup>2</sup>; im oldenburgischen Teil des Bistums Münster<sup>3</sup>)**

#### **Inhalt:**

#### **1.0 Aufgabe und Ziel**

#### **2.0 Arbeitsplatzcomputer**

- 2.1 Begriffsbestimmung
- 2.2 Gefahren durch den Einsatz von Arbeitsplatzcomputern

#### **3.0 Allgemeine Grundsätze**

- 3.1 Verantwortlichkeit der Mitarbeiter
- 3.2 Verantwortlichkeit der Dienststellenleiter
- 3.3 Technische und organisatorische Maßnahmen
- 3.4 Mindestanforderungen
- 3.5 Wahrung fremder Urheberrechte
- 3.6 Einsatz von Shareware und Public-Domain-Programmen
- 3.7 Weitere Maßnahmen

#### **4.0 Datenschutzklassen**

- 4.1 Datenschutzklasse I
- 4.2 Datenschutzklasse II
- 4.3 Datenschutzklasse III
- 4.4 Nicht zu speichernde Daten
- 4.5 Einordnung in die Datenschutzklassen
- 4.6 Geltung der jeweils höchsten Schutzklasse
- 4.7 Vermeidung der Mehrfachsicherung

#### **5.0 Nach den Datenschutzklassen erforderliche Maßnahmen**

- 5.1 Maßnahmen in Datenschutzklasse I
- 5.2 Maßnahmen in Datenschutzklasse II
- 5.3 Maßnahmen in Datenschutzklasse III

#### **6.0 Maßnahmen für besondere Gefahrenlagen**

- 6.1 Virenschutz
- 6.2 Schutz von Fernkommunikationsanlagen
- 6.3 Fernwartung
- 6.4 Wartungsarbeiten in den Räumen der Dienststelle
- 6.5 Wartungsarbeiten außerhalb der Dienststelle
- 6.6 Sicherung der Integrität der Datenbestände
- 6.7 Verbot privater Datenverarbeitung
- 6.8 Nutzung privater Datenverarbeitungssysteme zu dienstlichen Zwecken

---

1 für das Bistum Hildesheim veröffentlicht im Kirchlichen Anzeiger für das Bistum Hildesheim, Jahrgang 1994, Seite 413

2 für das Bistum Osnabrück veröffentlicht im Kirchlichen Amtsblatt für die Diözese Osnabrück, Band 50, Nr. 7, Seite 68 ff., Art. 81

3 für das Offizialat Vechta veröffentlicht im Kirchlichen Amtsblatt für die Diözese Münster, Jahrgang 1994, Seite 152 ff.

## **7.0 Maßnahmen zur Datensicherung**

7.1 Sicherungskopien der verwendeten Programme

7.2 Zeitabstände bei der Datensicherung

7.3 Ausdruck von Datenbeständen in Abwesenheit des zuständigen Mitarbeiters

7.4 Vernichtung von EDV-Ausdrucken und Datenträgern

## **8.0 Schlußbestimmungen**

### **1.0 Aufgabe und Ziel**

Diese Richtlinie regelt den Einsatz von Arbeitsplatzcomputern im Generalvikariat, den sonstigen diözesanen Dienststellen, den Pfarrämtern, Kirchengemeindeverbänden und Kirchenstiftungen und den sonstigen, der kirchlichen Aufsicht unterliegenden Einrichtungen in den Bistümern Hildesheim, Osnabrück sowie im oldenburgischen Teil des Bistums Münster und im Bischöflichen Amt Schwerin. Sie ist als Ergänzung zur Anordnung über den Kirchlichen Datenschutz (KDO) und den zu ihr ergangenen bereichsspezifischen Datenschutzregelungen in ihren jeweils geltenden Fassungen anzusehen.

### **2.0 Arbeitsplatzcomputer**

#### **2.1 Begriffsbestimmung**

Arbeitsplatzcomputer (APC) im Sinne dieser Richtlinie sind alle selbständigen Systeme der Informationstechnik, die einem Mitarbeiter zur Erfüllung seiner dienstlichen Aufgaben an seinem Arbeitsplatz zur Verfügung gestellt werden. Sie können als Einzelgerät (Stand-Alone-PC) oder in Verbindung mit anderen APC (Netzwerken) oder in Verbindung mit Anlagen der mittleren Datentechnik und Großcomputern (PC/HostKoppelung) installiert sein.

#### **2.2 Gefahren durch den Einsatz von Arbeitsplatzcomputern**

Arbeitsplatzcomputer verfügen über eine im Wesentlichen einheitliche Systemarchitektur sowie international genormte und standardisierte Bauteile und Schnittstellen. Ihre Betriebssysteme haben als Standardsoftware eine sehr weite Verbreitung. Es handelt sich bei ihnen daher um sogenannte „offene Systeme“, die jederzeit einen Anschluss weiterer APC ermöglichen und heute praktisch von jedermann bedient werden können. Zum Schutz des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die auf ihnen gespeicherten personenbezogenen Daten durch besondere Vorkehrungen vor unberechtigtem Zugriff sowie vor unberechtigter Verarbeitung und Nutzung zu schützen.

### **3.0 Allgemeine Grundsätze**

#### **3.1 Verantwortlichkeit der Mitarbeiter**

Jeder Mitarbeiter trägt die datenschutzrechtliche Verantwortung für eine vorschriftsgemäße Ausübung seiner Tätigkeit. Es ist ihm untersagt, personenbezogene Daten zu einem anderen, als in der jeweils rechtmäßigen Aufgabenerfüllung liegenden Zweck, zu verarbeiten oder zu offenbaren.

### **3.2 Verantwortlichkeit der Dienststellenleiter**

Die Leiter der jeweiligen Dienststellen und Einrichtungen tragen die Verantwortung für eine den Grundsätzen des Datenschutzes entsprechende Ausstattung der Arbeitsplatzcomputer. Bei der Neuanschaffung von APC müssen daher Konzepte zur datenschutzgerechten Ausgestaltung der Arbeitsplätze in die Investitionsentscheidung miteinbezogen werden.

### **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 zu § 5 KDO und die nach dieser Richtlinie 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:

- Die Datenverarbeitungsanlage ist unter Verwendung des hierzu erlassenen Musterformulars beim zuständigen Bischöflichen Beauftragten für den Datenschutz zum Register der automatisch betriebenen Dateien (§ 17 Abs. 3 KDO) anzumelden.
- Alle bei der Verarbeitung personenbezogener Daten tätigen hauptamtlichen und ehrenamtlichen Mitarbeiter haben die Verpflichtungserklärung gemäß § 4 Abs. 2 Satz 1 KDO abzugeben. Eine Durchschrift hiervon ist dem Bischöflichen Beauftragten für den Datenschutz zuzuleiten. Den Mitarbeitern, die die Verpflichtungserklärung unterschrieben haben, ist ein Abdruck der jeweils gültigen Anordnung über den Kirchlichen Datenschutz und der in ihrem Arbeitsbereich zu beachtenden bereichsspezifischen Datenschutzregelungen (Schulen, Krankenhäuser, Friedhöfe etc.) auszuhändigen.
- Der Kreis der Nutzungsberechtigten ist schriftlich festzulegen.
- Bei Einrichtungen und Organisationen, die ständig mehr als fünf Arbeitnehmer mit der automatischen Verarbeitung personenbezogener Daten beschäftigen, ist ein betrieblicher Datenschutzbeauftragter zu bestellen und dem Bischöflichen Beauftragten für den Datenschutz mit der Meldung zum Datenschutzregister zu benennen.
- 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.

### **3.5 Wahrung fremder Urheberrechte**

Auf Arbeitsplatzcomputern dürfen nur Originalversionen von Softwareprogrammen im Rahmen der Lizenzbedingungen des Herstellers eingesetzt werden. Die Anfertigung von Programmkopien zum Zwecke der Weitergabe an andere Dienststellen und Einrichtungen sowie zum Einsatz auf privaten PC ist aus urheberrechtlichen und strafrechtlichen Gründen strengstens untersagt (Raubkopieren). Die Stelle, die die Originalversion erworben hat, hat diese beim Hersteller ordnungsgemäß registrieren zu lassen.

### **3.6 Einsatz von Shareware und Public-Domain-Programmen**

Die im Handel erhältlichen Shareware und Public-Domain-Programme sind keine Originalprogramme sondern Kopien der Originalversionen. Durch die häufigen Kopiervorgänge und meist ungeprüften Disketten ist die Gefahr vor Virenbefall hier besonders groß. Darüber hinaus sind solche Programme oft unzureichend dokumentiert und ihre Kompatibilität mit anderen Programmen zweifelhaft. Aus diesen Gründen soll grundsätzlich auf den Einsatz solcher Programme verzichtet werden. Lässt sich ihr Einsatz im Einzelfall nicht vermeiden, so sind die Programme vor der Installation mit einem Viren-Scanner auf Virenbefall zu untersuchen. Ein dauerhafter Einsatz macht zudem eine Registrierung beim Hersteller erforderlich.

### **3.7 Weitere Maßnahmen**

Die Notwendigkeit, weitere Schutzmaßnahmen durchzuführen, richtet sich nach dem Grade der Schutzbedürftigkeit der gespeicherten personenbezogenen Daten. Liegen besondere Gefahrenlagen vor, sind in der Regel weitere Maßnahmen nach Ziffer 6 erforderlich.

## **4.0 Datenschutzklassen**

### **4.1 Datenschutzklasse I**

Zur Datenschutzklasse I gehören Daten, deren Missbrauch keine besondere Beeinträchtigung des Betroffenen erwarten lässt. Hierzu gehören Adressangaben, Berufs-, Branchen- oder Geschäftsbezeichnungen. Für sie sind die unter Ziffer 5.1 festgelegten Maßnahmen durchzuführen.

### **4.2 Datenschutzklasse II**

Zur Datenschutzklasse II gehören Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann. Hierzu gehören Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und Jubiläumsdaten, etc.. Für sie sind die unter Ziffer 5.2 festgelegten Maßnahmen durchzuführen.

### **4.3 Datenschutzklasse III**

Zur Datenschutzklasse III gehören Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann. Hierzu gehören Daten über kirchliche Amtshandlungen, gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen, die Mitgliedschaft in einer Religionsgesellschaft, arbeitsrechtliche Rechtsverhältnisse, Disziplinarentscheidungen, etc.. Für sie sind die unter Ziffer 5.3 festgelegten Maßnahmen durchzuführen.

### **4.4 Nicht zu speichernde 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 würde dem Vertrauen in die Verschwiegenheit katholischer Dienststellen und Einrichtungen schweren Schaden zufügen. Daher dürfen diese Daten nicht auf Arbeitsplatzcomputern verarbeitet werden.

## **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.

## **4.6 Geltung der jeweils höchsten Schutzklasse**

Gehören die auf einem Arbeitsplatzcomputer gespeicherten Daten unterschiedlichen Schutzklassen an, so richten sich die nach dieser Richtlinie zu treffenden Maßnahmen nach der höchsten, in der Datenverarbeitung vorkommenden Schutzklasse.

## **4.7 Vermeidung der Mehrfachsisicherung**

Schutzmaßnahmen nach den Datenschutzklassen II oder III machen die für die jeweils niedrigeren Schutzklassen vorgesehenen Maßnahmen gleicher Zielrichtung in

## **5.0 Nach den Datenschutzklassen erforderliche Maßnahmen**

### **5.1 Maßnahmen in Datenschutzklasse I**

Zum Schutz der in die Datenschutzklasse I einzuordnenden Daten sind in der Regel folgende Maßnahmen erforderlich:

- Die Inbetriebnahme des APC ist nur nach Eingabe eines benutzerdefinierten Kennwortes möglich, das in regelmäßigen Abständen erneuert werden sollte. Das Laden des Betriebssystems kann nicht von einem der installierten Diskettenlaufwerke aus erfolgen (Boot-Schutz). Im Mehrbenutzer- oder Netzwerkbetrieb und bei einer PC/Host-Koppelung ist zudem eine Rechteverwaltung auf Unterverzeichnis- und Dateiebene erforderlich, wenn nicht alle Nutzer berechtigt sein sollen, auf die personenbezogenen Daten Zugriff zu nehmen.
- Sicherungskopien und Ausdrücke der Datenbestände sind verschlossen, im Interesse der Dienststelle möglichst in feuerfesten Stahlschränken aufzubewahren.
- Nicht mehr benötigte Dateien sind so zu löschen, daß ihre Wiederherstellung ausgeschlossen ist (physikalisches Löschen).

### **5.2 Maßnahmen in Datenschutzklasse II**

Zum Schutz, der in die Datenschutzklasse II einzuordnenden Daten sind in der Regel folgende Maßnahmen erforderlich:

- Die auf der Festplatte gespeicherten Programme und Daten sollten dauerhaft so verschlüsselt werden, dass eine Entschlüsselung nur bezüglich solcher Programmteile und Daten stattfindet, die vom APC in den Hauptspeicher geladen werden (Online-Verschlüsselung). Der Zugang zum Entschlüsselungsprogramm ist nur nach Eingabe einer Benutzererkennung und eines Passwortes möglich, das vom Anwender in regelmäßigen Abständen zu erneuern ist. Dabei ist eine Begrenzung der Anmeldeversuche erforderlich. Das Hochfahren des APC vom Diskettenlaufwerk aus, ist auszuschließen.
- Anmeldeversuche am APC sind durch Einsatz geeigneter Programme zu protokollieren.

- bei Mehrbenutzer- und Netzwerkbetrieb ist eine abgestufte Rechteverwaltung für jeden Benutzer oder einzelne Benutzergruppen erforderlich. Der Zugang zum Betriebssystem sollte nur für den Systemverwalter möglich sein;
- Sicherungskopien sollten ebenfalls verschlüsselt und in abschließbaren, feuerfesten Schränken aufbewahrt werden; die Schnittstellen sind vor unberechtigtem Zugriff zu sichern.

### 5.3 Maßnahmen in Datenschutzklasse III

Zum Schutz, der in die Datenschutzklasse III einzuordnenden Daten sind in der Regel folgende Maßnahmen erforderlich:

- Die auf der Festplatte gespeicherten Programme und Daten sind dauerhaft zu verschlüsseln (OnlineVerschlüsselung). Eine Entschlüsselung findet nur bezüglich solcher Programme und Daten statt, die vom APC in den Hauptspeicher geladen werden. Der Zugang zum Entschlüsselungsprogramm ist nur nach Eingabe einer Benutzererkennung und eines zumindest achtstelligen Passwortes möglich, das vom Anwender in regelmäßigen Abständen zu erneuern ist. Trivialpasswörter (z.B. 4711, 12345, Gast, master) dürfen nicht verwendet werden. Dabei ist programmseitig eine Begrenzung der Anmeldeversuche auf höchstens drei Fehlversuche vorzusehen. Das Hochfahren des APC vom Diskettenlaufwerk aus, ist auszuschließen.
- im Mehrbenutzer- und Netzwerkbetrieb sind für jeden Benutzer abgestufte Rechte für den Zugriff auf Programme, Daten und Peripheriegeräte (insbes. Laufwerke, Schnittstellen) durch einen Systemverwalter zu vergeben; Systemaktivitäten sind durch eine hierfür geeignete Software zu protokollieren, deren Auswertung durch eine Person erfolgen sollte, die selbst nicht Systemverwalter ist.
- Sicherungskopien sind zu verschlüsseln und in verschlossenen, möglichst feuerfesten Stahlschränken aufzubewahren.

## 6.0 Maßnahmen für besondere Gefahrenlagen

Über die in den Ziffern 3 bis 5 genannten Anforderungen hinaus können im Einzelfall bei Vorliegen besonderer Gefahrenlagen, weitere Maßnahmen erforderlich sein.

### 6.1 Virenschutz

Bei Einsatz von APC in öffentlichen Fernkommunikationsnetzen (Telefax, Teletex u.ä.) sowie beim Anschluss von APC an externe Datenbanken ist ein ausreichender Schutz vor Virenbefall zu installieren. Aus Kosten- und Sicherheitsgründen ist hierfür in der Regel eine Hardwareerweiterung erforderlich. Sollte diese Möglichkeit wegen des Fehlens freier Steckplätze auf dem APC nicht gegeben sein, kann ausnahmsweise ein Softwareprogramm eingesetzt werden (VirenScanner), das regelmäßig auf den neuesten Stand zu bringen ist.

### 6.2 Schutz von Fernkommunikationsanlagen

APC, die an Einrichtungen der Fernkommunikation angeschlossen sind und mit deren Hilfe Daten der Schutzklasse III übertragen werden können, sind auch gegen Ausspähung durch Abhören des Leitungsnetzes zu sichern. Hierzu stehen abschirmsichere Kabel zur Verfügung. Die

Daten sind zudem in verschlüsselter Form zu übertragen. Das zur Entschlüsselung benötigte Passwort darf nicht auf dem gleichen Wege an den Empfänger übermittelt werden.

### **6.3 Fernwartung**

Eine Fernwartung von APC durch betriebsfremde Firmen schafft besondere Gefahren hinsichtlich der Ausspähung von Daten. Sie darf daher nur erfolgen, wenn zuvor durch Rückruf bei dem Fremdunternehmen die Berechtigung zur Vornahme von Wartungsarbeiten geklärt worden ist. Die Standleitung ist anschließend durch den für das System verantwortlichen Mitarbeiter zu aktivieren. Der Ablauf der Wartungsarbeiten und der dabei übermittelten Daten ist möglichst durch eine geeignete Software automatisch zu protokollieren und durch den Leiter der Dienststelle zu kontrollieren.

### **6.4 Wartungsarbeiten in der Dienststelle**

Bei der Durchführung von Wartungsarbeiten innerhalb der Dienststelle, ist in der Regel die ständige Anwesenheit des für das System verantwortlichen Mitarbeiters erforderlich. Dabei wird ein Zugriff auf Datenbestände durch den Wartungsdienst normalerweise nicht erforderlich sein. In diesen Fällen ist, je nach Datenschutzklasse durch Paßwortschutz und/oder Verschlüsselung sicherzustellen, dass der Wartungsdienst in diese Bereiche keinen Einblick erhält. In den anderen Fällen ist mit besonderer Sorgfalt darauf zu achten und nach Möglichkeit auch technisch sicherzustellen, dass keine Kopien der Datenbestände gefertigt werden können. Muss dem Wartungsdienst bei Vornahme der Arbeiten ein Passwort mitgeteilt werden, ist dieses sofort nach deren Beendigung zu ändern.

### **6.5 Wartungsarbeiten außerhalb der Dienststelle**

Die Durchführung von Wartungsarbeiten in den Räumen eines Fremdunternehmens kann nur in besonderen Ausnahmefällen gestattet werden. Die Gründe und die Art und Weise ihrer Durchführung sind schriftlich zu dokumentieren. Vor Herausgabe des APC ist dessen Festplatte zu verschlüsseln und eine Rechteverwaltung zu installieren, die der Werkstatt keine Zugriffsrechte auf sensible Datenbestände gestattet.

### **6.6 Sicherung der Integrität der Datenbestände**

Bei dem Einsatz von Datenbankprogrammen entstehen besondere Gefahren, wenn verschiedene Dateien miteinander verknüpft werden. In diesen Fällen hat eine Änderung von Datensätzen innerhalb einer Datei nicht immer auch eine Änderung in der mit dieser verknüpften Datei zur Folge. Hierdurch können sich in Bezug auf die gleiche Person Datenbestände unterschiedlichen Inhaltes ergeben. Von den Mitarbeitern wird in diesen Fällen besondere Aufmerksamkeit verlangt, um eine gleichmäßige Änderung des Datenbestandes an allen Stellen zu gewährleisten. Daher ist bei der Neuanschaffung von Datenbanken solchen Softwareprodukten der Vorzug zu geben, die eine Änderung von Datensätzen nur dann zulassen, wenn gleichzeitig auch die mit diesen verknüpften Datensätze geändert werden (referentielle Integrität).

## **6.7 Verbot privater Datenverarbeitung**

Unabhängig von der Einordnung der zu verarbeitenden Daten in die Datenschutzklassen der Ziffern 4.1 bis 4.3, ist eine private Erhebung, Verarbeitung und Nutzung dienstlicher Daten unzulässig.

## **6.8 Nutzung privater Datenverarbeitungssysteme zu dienstlichen Zwecken**

Die Nutzung privater Datenverarbeitungssysteme, Datenträger und Programme zu dienstlichen Zwecken ist nur erlaubt, wenn dieses zur Erfüllung der dem Anwender obliegenden dienstlichen Aufgaben unabweislich oder zwingend geboten ist. Hierfür bedarf es der schriftlichen Genehmigung der speichernden Dienststelle. Die Genehmigung darf nur erteilt werden, wenn der Eigentümer der Datenverarbeitungsanlage folgende schriftliche Erklärung abgegeben hat:

„Ich verpflichte mich, bei der Verarbeitung personenbezogener Daten auf meinem privaten Datenverarbeitungssystem, bzw. auf einem Datenverarbeitungssystem in meinen Privaträumen die Anordnung über den Kirchlichen Datenschutz - KDO - nebst Durchführungsbestimmungen und die Richtlinie zum Einsatz von Arbeitsplatzcomputern in den Bistümern Hildesheim, Osnabrück, im oldenburgischen Teil des Bistums Münster und im Bischöflichen Amt Schwerin einzuhalten. Eine Ausfertigung der KDO und der Richtlinien ist mir heute übergeben worden. Gleichzeitig unterstelle ich mich der Aufsicht des Bischöflichen Beauftragten für den Datenschutz und übernehme die der speichernden Dienststelle obliegenden Verpflichtungen nach § 17 Abs. 2 KDO.

Ich verpflichte mich weiter, der Dienststelle auf Anforderung die für die dienstlichen Zwecke verwendeten Datenträger sowie Ausdrucke aller gespeicherter Daten zur Verfügung zu stellen. Nach Beendigung der Zusammenarbeit werde ich nach Kräften an der Übertragung des Datenbestandes auf ein anderes dienstliches Datenverarbeitungssystem mitwirken. In diesem Falle werde ich auch alle dienstlich benötigten Datenträger und Ausdrucke an die Dienststelle herausgeben und dafür Sorge tragen, dass die Daten auf meiner Anlage vollständig so gelöscht werden, dass eine Wiederherstellung des Datenbestandes nicht mehr möglich ist.“

Der genehmigte Antrag und die schriftliche Verpflichtungserklärung sind in drei Stücken auszufertigen, von denen eines bei der Dienststelle und eines bei dem Verpflichteten verbleibt. Die dritte Ausfertigung ist dem Bischöflichen Beauftragten für den Datenschutz zur Kenntnisnahme zuzuleiten.

## **7.0 Maßnahmen zur Datensicherung**

Zum Schutz des Datenbestandes vor dessen Verlust sind regelmäßige Datensicherungen erforderlich.

### **7.1 Sicherungskopien der verwendeten Programme**

Die mit dem APC angelegten Datenbestände sind in der Regel nur mit den eingesetzten Softwareprogrammen wieder lesbar zu machen. Die Datensicherung muss sich daher auch auf diese Programme erstrecken. Aus diesem Grunde sind vor Beginn der Verarbeitung Sicherungskopien der verwendeten Programme anzulegen und möglichst von den Originaldisketten der Programme und den übrigen Datenträgern getrennt aufzubewahren.

## 7.2 Zeitabstände bei der Datensicherung

Der aktuelle Datenbestand sollte mindestens einmal täglich, bei Ende der Arbeit mit dem Datenverarbeitungssystem gesichert werden. Darüber hinaus sollte monatlich einmal eine Sicherung der gesamten Festplatte durchgeführt werden.

Kann der Verlust von Daten den Betroffenen in seinen Rechten beeinträchtigen (z.B. Personal- daten, kirchl. Amtshandlungsdaten), so ist die Zahl der Datensicherungen auf angemessene Abstände zu erhöhen. In diesen Fällen sind auch Zweitkopien der jeweiligen Sicherungskopien anzufertigen.

Bei dem Neuerwerb von Programmen zur Verarbeitung personenbezogener Daten soll nach Möglichkeit solchen Programmen der Vorzug gegeben werden, die eine automatische Sicherung des Datenbestandes durchführen.

## 7.3 Ausdruck von Datenbeständen in Abwesenheit des zuständigen Mitarbeiters

Sollen umfangreiche Ausdrücke von personenbezogenen Daten aus organisatorischen Gründen während der Abwesenheit des hierfür zuständigen Mitarbeiters erfolgen, so ist in geeigneter Weise dafür Sorge zu tragen, dass andere Mitarbeiter sowie betriebsfremde Personen während der Zeit, in denen die Ausdrücke unbeaufsichtigt sind, keinen Zugang zu den Räumen haben, in denen sich der APC und der Drucker befinden.

## 7.4 Vernichtung von EDV-Ausdrucken und Datenträgern

EDV-Ausdrücke mit personenbezogenen Daten sind durch Zerreißgeräte oder durch andere geeignete Maßnahmen, die die Lesbarkeit oder Wiederherstellbarkeit ausschließen, zu vernichten.

Datenträger (Disketten, Festplatten, Datenbänder, etc.), die nicht mehr benötigt werden, sind vor ihrer Beseitigung so zu löschen, bzw. zu behandeln, dass die Wiederherstellung, der auf ihnen gespeichert gewesenen Daten, ausgeschlossen ist. Dieses kann durch Neumagnetisierung der Datenträger, durch physikalisches Löschen der Dateien, Unterverzeichnisse und Verzeichnisse oder in anderer Weise geschehen.

## 8.0 Schlussbestimmungen

Diese Richtlinien sind von den Leitern der speichernden Stellen den hiervon betroffenen Mitarbeitern/innen auszuhändigen oder sonst in geeigneter Weise bekannt zu machen.

*Diese Richtlinien treten am 1.8.1994 in Kraft.<sup>1</sup>*

*Diese Richtlinien treten mit ihrer Verkündung im Amtsblatt der Diözese in Kraft.<sup>2</sup>*

*Mit Verkündung dieser Richtlinie treten die Richtlinien für den Einsatz von Informationstechnik sowie den Datenschutz am Arbeitsplatz in der Diözese Hildesheim vom 1. Juli 1991 außer Kraft.<sup>3</sup>*

Hildesheim, den 1. November 1994

Osnabrück, 27. Juli 1994

Vechta, den 9. August 1994

---

1 Text, der im Bistum Osnabrück verkündeten Fassung

2 Text, der im Offizialatsbezirk Vechta verkündeten Fassung

3 gilt nur im Bistum Hildesheim

## **Veröffentlichung von persönlichen Daten (z. B. Altersjubiläum) in Pfarrbriefen und ähnlichen Publikationen**

Nach § 3 Abs. 1 der Anordnung über den kirchlichen Datenschutz – KDO – (Kirchlicher Anzeiger 1994, Seiten 13, 14) ist die Verarbeitung und Nutzung personenbezogener Daten (also z. B. das Übermitteln, d. h. Bekanntgeben an Dritte) nur zulässig, soweit die KDO oder eine andere kirchliche oder eine staatliche Rechtsvorschrift dies erlaubt oder anordnet (1. Alternative) oder der Betroffene eingewilligt hat (2. Alternative).

Die Weitergabe personenbezogener Daten an Dritte (wie Banken, Tageszeitungen, Firmen u.s.w.), die die Information für gewerbliche Zwecke nutzen könnten, ist ohne schriftliche Einverständniserklärung des Betroffenen generell untersagt. Entsprechende Veröffentlichungen in kirchlichen Pfarrbriefen sind dagegen statthaft, nämlich die Information der Gemeinde und die Förderung der Gemeinschaft (Erläuterungen zum Datenschutz in den Pfarrgemeinden, Ziffer 3.5.3). Von einer Veröffentlichung besonderer Ereignisse (z. B. eines Geburtstages) in Verbindung mit der Anschrift des Betroffenen soll ohne seine vorherige schriftliche Einwilligung grundsätzlich abgesehen werden, da der Verdacht besteht, dass die Veröffentlichung der Anschrift von Jubilaren missbraucht wird und möglicherweise in Einzelfällen sogar zu kriminellen Handlungen geführt hat.

Jeder Betroffene kann gegen eine Veröffentlichung seiner personenbezogenen Daten Widerspruch erheben. Es wird deshalb empfohlen, vor einer Veröffentlichung vorsorglich zu prüfen, ob von einem Einverständnis des Betroffenen ausgegangen werden kann.

Auf das Widerspruchsrecht ist einmal jährlich, möglichst zu Beginn des Jahres, hinzuweisen (Pfarrbrief, Aushangkasten). Der Text dazu sollte folgenden Wortlaut haben:

„Im Pfarrbrief können Sakramentsspendungen, Alters- und Ehejubiläen, Geburten, Sterbefälle, Ordens- und Priesterjubiläen usw. mit Namen und ggf. mit Anschrift des Betroffenen sowie dem Tag und der Art des Ereignisses veröffentlicht werden, wenn der Betroffene nicht vorher schriftlich oder in sonstiger Form widersprochen hat. Widersprüche sollten dem Pfarramt schriftlich mitgeteilt werden.“

Hildesheim, den 8. Januar 1998

Bischöfliches Generalvikariat