RICHTLINIE FÜR DEN EINSATZ VON INFORMATIONSTECHNIK IN DER DIÖZESE LIMBURG

Grundlage für den Datenschutz in der Diözese Limburg ist die Anordnung über den kirchlichen Datenschutz (KDO) nebst Durchführungsbestimmungen zur KDO[1].

Aufgabe und Gegenstand des Datenschutzes im kirchlichen Bereich ist es, durch den Schutz personenbezogener Daten vor Missbrauch bei ihrer Speicherung, Übermittlung, Veränderung oder Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken. Die Anordnung über den kirchlichen Datenschutz schützt personenbezogene Daten, die vom Bistum, von den Kirchengemeinden, Kirchengemeindeverbänden und Kirchenstiftungen und von den ihrer Aufsicht unterstehenden kirchlichen Körperschaften, Stiftungen, Anstalten, Werken und Einrichtungen sowie im Auftrag dieser Stellen verarbeitet werden. Gemäß § 19 KDO werden zur Sicherstellung des Datenschutzes hiermit folgende Richtlinien erlassen:

§ 1 Geltungsbereich

1. Diese Richtlinie gilt für:
   - das Bistum, seine Behörden und seine Dienststellen,
   - die Kirchengemeinden, Kirchengemeindeverbände sowie Kirchenstiftungen,
   - den Diözesancaritasverband, die Bezirkscaritasverbände, ihre Untergliederungen und ihre Fachverbände ohne Rücksicht auf ihre Rechtsform,
   - die der kirchlichen Aufsicht unterliegenden Einrichtungen, Körperschaften, Stiftungen, Anstalten und Werke und sonstigen kirchlichen Rechtsträger ohne Rücksicht auf ihre Rechtsform,

   im nachfolgenden verantwortliche Stelle genannt.

   Diese Richtlinie gilt ergänzend zur „Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Limburg“ vom 14.07.1995 für die Katholischen Krankenhäuser in der Diözese Limburg.
2. Diese Richtlinie gilt für die Datenverarbeitung, insbesondere für die Verarbeitung personenbezogener Daten beim Einsatz von Datenverarbeitungssystemen, die speicherprogrammierbar sind und arbeitsplatzbezogen eingesetzt werden. Hierunter fallen Arbeitsplatzcomputer (APC), Mehrplatzsysteme, sonstige autonom betriebene Datenverarbeitungssysteme sowie die Verbindungen dieser Systeme untereinander oder mit anderen Rechnern. Ferner gilt diese Richtlinie für die Kommunikations- und Bürotechnik, soweit diese über das Niveau von Speicherschreibmaschinen hinausgeht.

§ 2 Verantwortlichkeit für die Einhaltung der Datenschutzvorschriften

1. Die verantwortliche Stelle hat die für sie geltenden Datenschutzbestimmungen zu beachten. Die verantwortliche Stelle trägt beim Einsatz von Datenverarbeitungssystemen die Verantwortung für die Durchführung der Datenschutzvorschriften. Die verantwortliche Stelle hat die erforderlichen technischen und organisatorischen Maßnahmen nach § 6 KDO und nach der Anlage zu § 6 KDO unverzüglich zu treffen sowie für die Durchführung des Datenschutzes Sorge zu tragen.
2. Die verantwortliche Stelle hat einen/eine Mitarbeiter/in als Verantwortlichen/Verantwortliche für das Datenverarbeitungssystem und die Einhaltung der Datenschutzvorschriften zu benennen.

[1] Amtblatt Nr. 11/2003, Seite 203ff.

§ 3 Nutzung privater und dienstlicher Hard- und Software

1. Eine private Erhebung, Verarbeitung und Nutzung dienstlicher Daten ist nicht zulässig.
2. Die Nutzung privater Datenverarbeitungssysteme, Datenträger und Programme zu dienstlichen Zwecken ist nur erlaubt, wenn dies zur Erfüllung der verantwortlichen Stelle obliegenden dienstlichen Aufgaben unabweislich oder zwingend geboten ist. Hierfür bedarf es der schriftlichen Genehmigung der Dienststelle. Grundsätzlich unzulässig ist die Nutzung von Datenverarbeitungssystemen der Dienststelle zu privaten Zwecken.
3. Die Nutzung von Datenverarbeitungssystemen zu dienstlichen Zwecken in Privaträumen bedarf der schriftlichen Genehmigung der Dienststelle.
4. Zusammen mit dem Antrag auf Erteilung der Genehmigung nach Abs. 2 und Abs. 3 hat der/die Mitarbeiter/in folgende schriftliche Verpflichtungserklärung abzugeben und diese der verantwortlichen Stelle zu übergeben:

   Verpflichtungserklärung

   „Ich verpflichte mich, bei der Verarbeitung personenbezogener kirchlicher Daten auf meinem privaten Datenverarbeitungssystem, bzw. auf einem Datenverarbeitungssystem in meinen Privaträumen
   - die Anordnung über den kirchlichen Datenschutz (KDO) nebst Durchführungsbestimmungen zur KDO einzuhalten,
   - die Richtlinie für den Einsatz von Informationstechnik in der Diözese Limburg einzuhalten und der verantwortlichen Stelle einen Ausdruck von allen gespeicherten Daten zur Verfügung zu stellen, wenn ein Antrag auf Auskunft nach § 13 der Anordnung über den kirchlichen Datenschutz (KDO) gestellt wird.

   Mir ist lediglich gestattet, folgende personenbezogene kirchliche Daten zu verarbeiten: ..... .

   Mir ist bekannt, dass ich mit einer datenschutzrechtlichen Überprüfung durch den kirchlichen Datenschutzbeauftragten rechnen muss. Ich unterstelle mich daher ausdrücklich auch dem kirchlichen Datenschutzbeauftragten einschließlich seiner Weisungen, die mit meiner Dienststelle abgestimmt sind.

   Name, Adresse, Standort des privaten Datenverarbeitungssystems, Unterschrift."

   Der schriftlich genehmigte Antrag und die schriftliche Verpflichtungserklärung sind bei der verantwortlichen Stelle aufzubewahren. Eine Kopie des genehmigten Antrages ist dem/der Mitarbeiter/in auszuhändigen. Eine Kopie des genehmigten Antrages leitet die verantwortliche Stelle dem kirchlichen Datenschutzbeauftragten zu.
5. Auf dem PC dürfen nur Originalprogramme und erlaubte Kopien eingesetzt werden. Da Computerprogramme unter den besonderen Schutz des Urheberrechtsgesetzes gestellt sind, ist vorbehaltlich einer urheberrechtlichen Zulässigkeit das Kopieren von Programmen oder die Weitergabe an interne und externe Personen und Stellen verboten. Erforderlich und erlaubt ist das Erstellen einer Sicherungskopie des Programms.
6. Die private Erhebung, Verarbeitung oder Nutzung dienstlicher Daten ist unzulässig.
7. Die Nutzung privater Datenverarbeitungssysteme, Datenträger und Programme zu dienstlichen Zwecken ist mit schriftlicher Genehmigung der zuständigen Dienststelle nur erlaubt, wenn dies zur Erfüllung der dem Anwender obliegenden dienstlichen Aufgaben unabweislich oder zwingend geboten ist. Dies gilt nicht für Daten des kirchlichen Meldewesens. Das Erfordernis der dienstlichen Genehmigung gilt ebenfalls für die Nutzung von Datenverarbeitungssystemen zu dienstlichen Zwecken außerhalb der Diensträume.

§ 4 Behandlung und Aufbewahrung von Datenträgern

1. Bewegliche Datenträger, die personenbezogene Daten oder Programme enthalten, sind dem Datenverarbeitungssystem nach Arbeitsende zu entnehmen und so ver-

schlossen aufzubewahren, dass ein unberechtigter Zugriff durch Dritte ausgeschlossen ist. Sobald die Daten zur Erfüllung der Aufgaben der speichernden Stelle nicht mehr benötigt werden, sind die personenbezogenen Inhalte von Datenträgern so zu zerstören (physisches Löschen), dass ihr Inhalt nicht rekonstruierbar ist.

2. Die auf Datenträger gespeicherten personenbezogenen Daten sind so zu verschlüsseln (Datenchiffrierung), dass eine Identifikation durch Unbefugte ausgeschlossen ist.
3. Das Kopieren von Datenträgern bzw. einzelnen Dateien ist nur zum Zwecke der Datensicherung, der Programmpflege, in Ausnahmefällen für Testläufe sowie zur Weitergabe an Dritte aus unabweislichen dienstlichen Gründen bei gleichzeitiger Beachtung der einschlägigen datenschutzrechtlichen Bestimmungen zulässig.
4. Vor Wartungsmaßnahmen an Datenverarbeitungsanlagen und an Datenträgern (z. B.: an Festplatten), sind die Dateien grundsätzlich zu löschen. Sofern eine vollständige Löschung nicht möglich ist und/oder Daten für die Fehleranalyse zur Verfügung gestellt werden, muss die wartende Stelle schriftlich verpflichtet werden, die Daten nicht unbefugt zu verarbeiten. Der Zugriffschutz bei Fernwartung muss im Einzelfall gesondert geregelt werden.

§ 5 Technische und organisatorische Maßnahmen

1. Es sind technische und organisatorische Maßnahmen zu treffen, deren Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Der Grad der Schutzbedürftigkeit bei der Verarbeitung personenbezogener Daten ergibt sich insbesondere aus
   - der Art der personenbezogenen Daten,
   - dem Zusammenhang und
   - dem Zweck ihrer Verarbeitung sowie
   - dem anzunehmenden Missbrauchsinteresse.

   Außerdem ist er abhängig von der Art des eingesetzten Datenverarbeitungssystems.
2. Die verantwortliche Stelle selbst hat dafür Sorge zu tragen,
   - dass der/die Mitarbeiter/in die Verpflichtungserklärung nach § 4 KDO und ggf. die Verpflichtungserklärung nach § 3 Ziffer 4 dieser Richtlinie unterzeichnet,
   - eine Übersicht über die Art der gespeicherten personenbezogenen Daten und über die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist sowie über deren regelmäßige Empfänger nach § 3a Abs. 2 KDO geführt wird,
   - die von ihnen automatisch betriebenen Dateien gemäß § 18b Abs. 2 i. V. mit § 3a Abs. 2 KDO beim kirchlichen Datenschutzbeauftragten gemeldet werden.
3. Es ist schriftlich festzulegen, wer das Datenverarbeitungssystem benutzen darf (Benutzungsberechtigte). Zur Realisierung der Zugangs- und Zugriffskontrolle ist mindestens zu gewährleisten, dass
   - bei Darstellung personenbezogener Daten auf Bildschirm oder Druckern Unbefugten die Einsicht verwehrt wird und
   - der Arbeitsraum und die Geräte oder Teile der Geräte bei Abwesenheit der Nutzungsberechtigten abgeschlossen sind.
4. Bei einer Neuanschaffung ist das Datenverarbeitungssystem zur Realisierung einer wirksamen Speicher-, Benutzer-, Zugriffs- und Übermittlungskontrolle mit einem Betriebsschloss / Passwort auszustatten.

   Falls der Grad der Schutzbedürftigkeit der Verarbeitung der Daten es erfordert, ist das eingesetzte Datenverarbeitungssystem mit einem Betriebssystem, das die individuelle Benutzeridentifikation und eine differenzierte Zugriffsberechtigung ermöglicht und/oder mit einer Zugriffschutz-Software, die neben diesem Leistungsspektrum auch eine Protokollierung und eine Menüsteuerung zulässt, auszustatten. Jeder/jede Mitarbeiter/in darf nur auf die Daten Zugriff haben, die er/sie im Rahmen seiner/ihrer Aufgaben benötigt.

Der Zugriffschutz bei Rechnerverbindungen und Mehrplatzsystemen muss im Einzelfall geregelt werden.

5. Protokollierungsdaten nach Ziff. 4 dienen ausschließlich den Zwecken der Datenschutzkontrolle. Sie dürfen nur von dem/der Benutzungsberechtigten, soweit es sich um ihn/sie betreffende Daten handelt sowie dem kirchlichen Datenschutzbeauftragten gemeinsam mit dem/der Benutzungsberechtigten oder dem Dienstvorgesetzten der verantwortlichen Stelle eingesehen werden.
6. Unabhängig vom Grad der Schutzbedürftigkeit der Daten sind dabei zumindest folgende Maßnahmen zu treffen:
   (1) Alle mit Datenverarbeitung beauftragten Personen sind verpflichtet,
      a) nur mit den Programmen, Verzeichnissen (Ordnern) und Dateien auf den Datenverarbeitungsanlagen ihrer Dienststelle zu arbeiten, die von ihrem Dienstgeber für sie freigegeben und zur Verfügung gestellt worden sind,
      b) Passwörter nicht an Dritte weiterzugeben,
      c) sich nicht unter einem anderen Passwort, das ihnen bekannt geworden ist und für das sie keine Berichtigung haben, in das Informationstechnik-System einzuloggen oder Programm auszuführen,
      d) keine dienstfremden Datenträger in die Laufwerke der Datenverarbeitungsanlagen ihrer Dienststelle einzulegen (z. B. private Programme, Spiele, Demo-Disketten etc.) oder über sonstige Kommunikationsschnittstellen (z. B. USB, IrDa, Netzwerk, Firewire, etc.) mit der DV-Anlage zu verbinden oder verfügbar zu machen,
      e) an Programmdateien oder Programmeinstellungen keine Veränderungen vorzunehmen, die einer üblichen Nutzung als Anwender widersprechen,
      f) keine Änderungen der Installation (insbesondere Netzadressen, Programme, Verzeichnisse / Ordner, Zugriffsrechte, etc.) vorzunehmen,
      g) nicht unberechtigt über Datenfernverbindungen (z. B.: Telefonnetz) betriebsfremde Daten bzw. Programme in den Arbeits- oder Festspeicher (Festplatte, Diskette, USB-Speichermedien etc.) der Datenverarbeitungsanlage ihrer Dienststelle zu übertragen,
      h) keine Daten auf andere, dienstfremde Datenträger unberechtigt zu übertragen oder dienstfremden Personen unberechtigt zur Verfügung zu stellen,
      i) ohne Zustimmung des Berechtigten keine Vervielfältigung jeglicher Art von Handbüchern, technischen Datenblättern etc. oder von Auszügen daraus vorzunehmen und für private oder dienstfremde Zwecke zu verwenden,
      j) den PC und Peripheriegeräte nicht zu öffnen (z. B. aufzuschrauben) und keine hardwaremäßigen Veränderungen, auch nicht an der Verkabelung, vorzunehmen, es sei denn, dass sie von ihrem Dienstgeber im Rahmen von Wartungsarbeiten damit beauftragt worden sind,
      k) unberechtigten Zugriff bei vorübergehender Abwesenheit vom Arbeitsplatz auszuschließen, indem der PC in Pausen gesperrt oder abgemeldet wird, bei Dienstende eine Abmeldung oder - nach Möglichkeit - ein Herunterfahren des Systems vorgenommen wird.
   (2) Es ist schriftlich festzulegen, wer das Datenverarbeitungssystem benutzen darf (Benutzungsberechtigte).
   (3) Es ist sicherzustellen, dass bei Darstellung personenbezogener Daten auf Ausgabegeräten (Bildschirme, Drucker, Beamer, etc.) Unbefugten die Einsicht verwehrt wird.
   (4) Zur Realisierung der Zugangs- und Zugriffskontrolle ist zu gewährleisten, dass der Arbeitsraum und die Geräte bei Abwesenheit der Benutzungsberechtigten abgeschlossen bzw. nicht betriebsbereit sind.

7. Die angeschaffte System- und Anwendungssoftware darf aufgrund der hierüber abgeschlossenen Einzellizenzverträge nur auf dem hierfür bestimmten PC verwendet werden. Eine Übertragung auf einen anderen Computer ist untersagt.
8. Im Umgang mit Laptops, PDAs und Heimarbeitsplätzen ist besonders Sorge zum Datenschutz zu tragen.
9. Es ist untersagt, andere als vom Dienstgeber zur Verfügung gestellte Programme in das von ihm angeschaffte Gerät zu installieren. Insbesondere das Auftreten von Computerviren ist zu verhindern.

§ 6 Behandlung und Aufbewahrung von Datenträgern

1. Datenträger, die personenbezogene Daten oder Programme enthalten, sind so verschlossen aufzubewahren, dass ein unberechtigter Zugriff durch Dritte ausgeschlossen ist. Sobald die Daten zur Erfüllung der Aufgaben der verantwortlichen Stelle nicht mehr benötigt werden, sind die personenbezogenen Inhalte von Datenträgern so zu zerstören, dass ihr Inhalt nicht rekonstruierbar ist (physikalisches Löschen); gesetzliche Aufbewahrungsvorschriften und Archivierungsvorschriften des Dienstgebers sind dabei zu beachten.
2. Das Kopieren von Datenträgern bzw. einzelnen Dateien oder Programmen ist nur zum Zwecke der Datensicherung, der Programmpflege, in Ausnahmefällen für Testläufe sowie Weitergabe an Dritte aus unabweislichen dienstlichen Gründen bei gleichzeitiger Beachtung der einschlägigen datenschutzrechtlichen Bestimmungen zulässig.
3. An Programmen dürfen keine Veränderungen vorgenommen werden, die einer üblichen Nutzung als Anwender widersprechen.
4. Es dürfen weder Daten noch Programme auf andere dienstfremde Datenträger unberechtigt übertragen werden.

§ 7 Datenschutzgerechte Vernichtung von EDV-Ausdrucken und Datenmaterial

1. Bei EDV-Ausdrucken und Datenmaterial ist darauf zu achten, dass unbefugte Dritte nicht von den personenbezogenen Daten Kenntnis nehmen können. EDV-Ausdrucke und Datenmaterial sind in geeigneter, dem Datenschutz Rechnung tragender Weise in verschließbaren Behältnissen (z. B. Schränken) aufzubewahren. Gesetzliche Aufbewahrungsvorschriften und Archivierungsvorschriften des Dienstgebers sind dabei zu beachten.
2. Alle EDV-Ausdrucke und sämtliches sonstiges Datenmaterial sind datenschutzgerecht (z. B. Zerreißgeräte, etc.) zu vernichten, sobald diese zur Erfüllung der Aufgaben der verantwortlichen Stelle nicht mehr benötigt werden.
3. Datenträger (Disketten, Festplatten, Datenbänder etc.), die nicht mehr benötigt werden, sind vor ihrer Beseitigung zu löschen oder zu zerstören, um die Wiederherstellung der auf ihnen gespeicherten Daten auszuschließen.
4. Vernichtung kann auch in der Weise geschehen, dass die Datenträger oder sonstiges Datenmaterial einer dafür geeigneten Stelle zur Vernichtung übergeben werden. Über die Vernichtung ist ein Zertifikat auszustellen und der zuständigen Dienststelle auszuhändigen.

§ 8 Zugriffsschutz bei Fernwartung

1. Zur Datensicherheit muss gewährleistet sein, dass ein Zugriff auf den PC eines Mitarbeiters via Fernwartung (= Darstellung des Bildschirms beim EDV-Sachbearbeiter) nicht ohne Zustimmung oder Beteiligung des aktuell angemeldeten Benutzers erfolgen kann. Nach Abschluss der Fernwartung ist die Verbindung zu deaktivieren. Ein Neustart des PCs muss die Verbindung ebenfalls automatisch deaktivieren. Dies gilt i. d. R. nicht für Server-Systeme, die durch die ITAbteilung regelmäßig ferngewartet werden.
2. Bei der Fernwartung darf nur auf spezielle, vorher festgelegte Programme bzw. deren Daten zugegriffen werden, für die eine Fernwartung vereinbart wurde.
3. Der Ablauf der Wartungsarbeiten ist möglichst zu protokollieren.

4. Betriebsfremde Firmen müssen die Einhaltung der kirchlichen Datenschutzvorschriften gewährleisten.

§ 9 Telefaxgeräte

1. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihrer näheren Umstände. Verstöße gegen das Fernmeldegeheimnis können nach § 206 StGB mit Strafe geahndet werden.
2. Allen im Telefax-Verkehr eingesetzten Bediensteten und Zugriffsberechtigten ist untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen.
3. Bei der Versendung von Telefaxsendungen (z. B. vertrauliche Daten oder Dokumente) ist besondere Sorgfalt geboten, da diese beim Empfänger offen ankommen.
4. Bei der Übermittlung personenbezogener Daten, insbesondere solcher, die besonders schutzbedürftig sind (z. B. religiöse oder politische Anschauung, arbeitsrechtliche, finanzielle oder gesundheitliche Verhältnisse, strafbare Handlungen) ist Vorsorge zu treffen, um die Rechte der Betroffenen zu wahren. Sie sollen nur dann per Telefax übermittelt werden, 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 über die persönliche Entgegennahme der Sendung zu treffen.
5. Jeder Sendung sollte ein Vorblatt oder ein spezieller Telefax-Kopf beigefügt werden, der den Absender, dessen Telefax- und Telefonnummer, den Adressaten und die Anzahl der zu sendenden Seiten erkennen lässt.
6. Die Telefaxnummer des Empfängers ist sorgfältig zu überprüfen. Zweifel an der Gültigkeit der Anschlussnummer sind vor Absendung des Telefax auszuräumen.
7. Telefax-Geräte sollen in solchen Räumen untergebracht werden, in denen gewährleistet ist, dass Telefax-Sendungen nicht unbeobachtet ankommen und von Unbefugten entnommen oder eingesehen werden können.

§ 10 Nutzung von E-Mail und Internet

1. Da im Internet keine Maßnahmen zur Sicherstellung der Integrität, Vertraulichkeit und Authentizität der übertragenen Informationen und des Kommunikationspartners getroffen wurden, sind entsprechende Regelungen erforderlich, die die damit verbundenen datenschutzrechtlichen und sicherheitsrelevanten Aspekte berücksichtigen. Diese werden vornehmlich in Dienstanweisungen oder Dienstvereinbarungen umgesetzt.
2. Rechtsverbindliche Vorgänge und Erklärungen, die einer besonderen Form bedürfen, sowie Vorgänge mit hohem Vertraulichkeitsgrad sollen nicht per elektronischer Post abgegeben werden, solange kein sicheres Verschlüsselungsverfahren besteht.
3. Die verantwortlichen Stellen sowie die Mitarbeiter/innen sind bei der Nutzung von e-Mail und Internet für die Sicherstellung des Datenschutzes verantwortlich.

§ 11 Abschließende Bestimmungen und Inkrafttreten

1. Diese Richtlinie ist von den Leitern der verantwortlichen Stellen den hiervon betroffenen Mitarbeitern auszuhändigen oder in geeigneter Weise vollständig bekannt zu geben.
2. Diese Richtlinie tritt am 01. Januar 2006 in Kraft; die Richtlinie vom 25. September 2003 wird aufgehoben.

Limburg, 21. Dezember 2005
Az.: 555 T/05/12/2

Dr. Günther Geis
Generalvikar