Ausführungsbestimmungen zum Datenschutz beim Einsatz von Informationstechnik

Gemäß § 19 der Anordnung über den kirchlichen Datenschutz – KDO – vom 01.10.2003 (Kirchliches Amtsblatt Münster 2003, Art. 234) werden zur Sicherstellung des Datenschutzes beim Einsatz von Informationstechnik für das Bistum Münster, nordrhein-westfälischer Teil, folgende Ausführungsbestimmungen erlassen:

§ 1 – Geltungsbereich

1. Diese Ausführungsbestimmungen gelten für die Verarbeitung personenbezogener Daten beim Einsatz von Informationstechnik (IT) durch die in § 1 Abs. 2 KDO genannten kirchlichen Rechtsträger. Hierunter fallen Arbeitsplatzcomputer (PC), Mehrplatzsysteme, sonstige autonom betriebene Datenverarbeitungssysteme sowie die Verbindung dieser Systeme untereinander oder mit anderen Systemen.
   PC im Sinne dieser Ausführungsbestimmungen 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, im Netzwerk mit anderen PCs oder in Verbindung mit Servern und/oder Großrechnern („Host“) installiert sein oder auf diese zugreifen.
2. Ferner gelten diese Ausführungsbestimmungen sinngemäß für die entsprechende Kommunikations- und Bürotechnik.

§ 2 – Verantwortlichkeit für die Einhaltung von Datenschutzvorschriften

1. Die verantwortliche Stelle (§ 2 Abs. 8 KDO) hat die für sie geltenden Datenschutzbestimmungen zu beachten. Sie trägt beim Einsatz von Datenverarbeitungssystemen die Verantwortung für die Durchführung der Datenschutzvorschriften. Sie hat die erforderlichen technischen und organisatorischen Maßnahmen gemäß § 6 KDO in Verbindung mit der Anlage hierzu unverzüglich zu treffen.
   Die Daten sind regelmäßig zu sichern („Backup“) oder an einer zentralen Stelle abzulegen, die zentral gesichert wird (z.B. Server / zentrale Datenablage bei der für die Datenverarbeitungssysteme zuständigen Gruppe).
2. Die Mitarbeiter tragen die datenschutzrechtliche Verantwortung für die vorschriftsmäßige Ausübung ihrer Tätigkeit. Es ist ihnen untersagt, personenbezogene Daten zu anderen als in der jeweils rechtmäßigen Aufgabenerfüllung liegenden Zwecken zu verarbeiten oder zu offenbaren.
3. Die für die verantwortliche Stelle Zuständigen und die für den Einsatz der Datenverarbeitungssysteme verantwortlichen Leiter haben für eine den Grundsätzen des Datenschutzes entsprechende Ausstattung zu sorgen.

§ 3 – Technische und organisatorische Maßnahmen

1. Es sind technische und organisatorische Maßnahmen zu treffen, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen. Der Grad der Schutzbedürftigkeit bei der Verarbeitung personenbezogener Daten ergibt sich insbesondere aus
   a) der Art der personenbezogenen Daten (z. B. kirchliche Amtshandlungen, gesundheitliche Verhältnisse, arbeitsrechtliche Verhältnisse),
   b) dem Zusammenhang mit anderen gespeicherten Daten,
   c) dem Zweck ihrer Verarbeitung und
   d) der Missbrauchsgefahr.

Außerdem ist er abhängig von der Art des eingesetzten Datenverarbeitungssystems.

2. Unabhängig vom Grad der Schutzbedürftigkeit der Daten sind dabei zumindest folgende Maßnahmen zu treffen:
    1. Alle mit Datenverarbeitung beauftragte 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 anderem Passwort, das ihnen bekannt geworden ist und für das sie keine Berechtigung haben, in das Informationstechnik-System einzuloggen oder Programme 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.
3. 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.

4. Im Umgang mit Laptops, PDAs und Heimarbeitsplätzen ist besondere Sorge zum Datenschutz zu tragen.
5. 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.

§ 4 – 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 zur 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.

§ 5 – Nutzung privater und dienstlicher Hard- und Software

1. 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.
2. Die private Erhebung, Verarbeitung oder Nutzung dienstlicher Daten ist unzulässig.
3. 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.

§ 6 – Datenschutzgerechte Vernichtung von EDV-Ausdrucken und Datenmaterial

1. Bei EDV-Ausdrucken oder sonstigem Datenmaterial ist darauf zu achten, dass diese datenschutzgerecht vernichtet werden, sobald diese zur Erfüllung der Aufgaben der verantwortlichen Stelle nicht mehr benötigt werden; gesetzliche Aufbewahrungsvorschriften und Archivierungsvorschriften des Dienstgebers sind dabei zu beachten.
2. 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.
3. Die 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.

§ 7 – 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 IT-Abteilung 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.

§ 8 - 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.

§ 9 – 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 damit verbundene 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.

§ 10 – Schlussbestimmungen

1. Die Ausführungsbestimmungen sind von den Verantwortlichen der zuständigen Dienststellen den hiervon betroffenen Mitarbeitern auszuhändigen oder sonst in geeigneter Weise bekannt zu geben.
2. Diese Ausführungsbestimmungen treten mit dem Datum ihrer Veröffentlichung im Kirchlichen Amtsblatt in Kraft. Gleichzeitig treten die Ausführungsbestimmungen zum Datenschutz beim Einsatz von Informationstechnik und die Ausführungsbestimmungen zum Datenschutz bei der Übermittlung personenbezogener Daten über Telefaxgeräte vom 01.04.1998 (KA Münster 1998, Nr. 11, Art. 119, Art. 120) außer Kraft.

Münster, den 1. September 2005

N. Kleyboldt
Generalvikar