

5.2 Fremdzugriffe

Der Zugriff aus und von anderen Datenverarbeitungsanlagen durch Externe (z. B. Fremdfirmen, fremde Dienststellen) schafft besondere Gefahren hinsichtlich der Ausspähung von Daten. Minimalanforderung ist eine Verpflichtung des Externen auf die KDO. Art und Umfang der Zugriffe sind auf ein Mindestmaß zu reduzieren und gesondert zu regeln. Für die Fernwartung gilt § 8 KDO entsprechend.“

Nr. 194

IT-Richtlinien zur Umsetzung von Ziffer IV. Anlage 2 zu § 6 KDO der Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO)

IT-Richtlinien zur Umsetzung von Ziffer IV. Anlage 2 zu § 6 KDO der Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO)

Präambel

Die IT-Richtlinien definieren einen Mindeststandard für den kirchlichen Datenschutz. Dieser dient auch dazu, die überdiözesane Zusammenarbeit zu erleichtern (Datenschutzkonformität). Die zu etablierenden Datenschutzklassen (DSK) sind sowohl auf personenbezogene als auch auf schützenswerte nicht personenbezogene Daten anzuwenden (z. B. auf Buchhaltungsdaten (= DSK II) und Kirchensteuerdaten (= DSK III)).

1. Nach den jeweiligen Datenschutzklassen erforderliche Maßnahmen

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

2. Maßnahmen in den Datenschutzklassen

2.1 Maßnahmen in Datenschutzklasse I

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

- Der Arbeitsplatzcomputer (APC) ist nicht frei zugänglich, z. B.: in einem abschließbaren Gebäude oder unter ständiger Aufsicht.
- Die Anmeldung am APC ist nur nach Eingabe eines benutzerdefinierten Kennwortes möglich.

II. Inkrafttreten

Die Regelungen in Abschnitt I treten am 1. September 2016 in Kraft.

Trier, den 30. August 2016

(Siegel)

Msgr. *Dr. Georg Bätzing*
Bischöflicher Generalvikar

- Sicherungskopien der Datenbestände sind verschlossen aufzubewahren.
- Vor der Weitergabe eines Datenträgers für einen anderen Einsatzzweck sind die auf ihm befindlichen Daten so zu löschen, dass ihre Wiederherstellung ausgeschlossen ist.
- Nicht öffentlich verfügbare Daten sind nur dann weiterzugeben, wenn sie durch geeignete Schutzmaßnahmen geschützt sind. Die Art und Weise des Schutzes ist vor Ort zu definieren.

2.2 Maßnahmen in Datenschutzklasse II

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

- Die Anmeldung am APC ist nur nach Eingabe eines benutzerdefinierten Kennwortes möglich, dessen Erneuerung in regelmäßigen Abständen systemseitig vorgesehen werden muss.
- Das Laden des Betriebssystems der Datenverarbeitungsanlage darf nur mit dem dafür bereitgestellten Betriebssystem erfolgen (Boot-Schutz). Diese BIOS-Einstellung ist durch ein besonderes Passwort zu sichern, das nur dem Systemverwalter bekannt ist.
- Im Mehrbenutzer- oder Netzwerkbetrieb und bei einer PC/Host-Koppelung ist eine abgestufte Rechteverwaltung erforderlich. Der Anwender sollte keine Administrationsrechte erhalten.
- Sicherungskopien und Ausdrücke der Datenbestände sind vor Fremdzugriff und vor der gleichzeitigen Vernichtung mit den Originaldaten zu schützen.
- Die Daten der Schutzklasse II sind auf zentralen Systemen in besonders gegen unbefugten Zutritt ge-

sicherten Räumen zu speichern, sofern keine begründeten Ausnahmefälle gegeben sind. Die jeweils beteiligten Systeme und Transportwege sind nach dem aktuellen Stand der Technik angemessen zu schützen.

- Eine Speicherung auf mobilen Datenträgern darf nur erfolgen, wenn diese mit einem geeigneten Zugriffsschutz ausgestattet sind.

2.3 Maßnahmen in Datenschutzklasse III

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

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

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

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

3. Maßnahmen zur Datensicherung

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

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

3.1 Sicherungskopien der verwendeten Programme

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

3.2 Zeitabstände bei der Datensicherung

Die Datensicherung soll in Umfang und Zeitabstand

anhand der entstehenden Auswirkungen eines Verlustes der Daten festgelegt werden.

4. Besondere Gefahrenlagen

4.1 Fernwartung

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

4.2 Auftragsdatenverarbeitung

Werden personenbezogene Daten auf zentralen Systemen außerhalb des Geltungsbereiches der Anordnung über den kirchlichen Datenschutz (KDO) gespeichert (z. B. Public Cloud), sind die Auftragnehmer auf die KDO zu verpflichten. Ergänzend ist sicherzustellen, dass der physikalische Speicherort der Daten ausschließlich im Geltungsbereich des BDSG liegt. Sobald eine einheitliche europäische Datenschutzverordnung in Kraft ist, wird auf deren Geltungsbereich abgestellt.

4.3 Nutzung privater Datenverarbeitungssysteme

Werden im zu genehmigenden Einzelfall personenbezogene Daten auf privaten Datenverarbeitungsanlagen verarbeitet oder werden personenbezogene Daten auf private E-Mail-Konten geleitet, sind die Nutzer schriftlich auf die Einhaltung dieser IT-Richtlinie zu verpflichten. In dieser Erklärung verpflichten sich die Nutzer, betreffende personenbezogene Daten durch die Dienststelle und auf deren Anforderung löschen zu lassen. Ergänzend soll dem Nutzer eine spezifische Handlungsanleitung ausgehändigt werden, um den Schutz dieser Daten zu gewährleisten.

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

4.4 Wartungsarbeiten in der Dienststelle durch externe Auftragnehmer

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

4.5 Wartungsarbeiten außerhalb der Dienststelle

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

4.6 Verschrottung und Vernichtung von Datenträgern

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

4.7 Passwortlisten der Systemverwaltung

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

5. Inkrafttreten

Die IT-Richtlinien zur Umsetzung von Ziffer IV. Anlage 2 zu § 6 KDO der KDO-DVO treten am 1. September 2016 in Kraft.

Trier, den 30. August 2016

(Siegel)

Msgr. *Dr. Georg Bätzing*
Bischöflicher Generalvikar

Nr. 195

Veröffentlichung von Weihe- und Geburtstagsjubiläen

Das Bistum beabsichtigt, zur Information über Weihe- und Geburtstagsjubiläen folgende Daten von im Bistum Trier tätigen Diakonen und Priestern wie bisher üblich in der Januar-Ausgabe des Paulinus zu veröffentlichen:

Name, Vorname, Geburtsdatum, Weihedatum und Anschrift.

Aus Gründen des kirchlichen Datenschutzes wird diese Absicht hiermit bekannt gemacht. Betroffene, die mit der Veröffentlichung ihrer personenbezogenen

Daten nicht einverstanden sind, mögen diesen entgegenstehenden Willen **bis spätestens 30. November 2016** schriftlich der zuständigen Abteilung (Zentralbereich 1.2 Seelsorge und pastorales Personal) mitteilen.

Sofern bis zu diesem Datum kein Widerspruch erhoben wurde, werden die Daten veröffentlicht werden.

Trier, den 19. September 2016

Das Bischöfliche Generalvikariat

Nr. 196

Kollekte am Allerseelentag

Die Kollekte am Allerseelentag (**Mittwoch, 2. November**) dient seit Jahren der Unterstützung der Priesterausbildung (Diözesan- und Ordenspriester) in Mittel- und Osteuropa. Für den Wiederaufbau der Kirche in den ehemals kommunistischen Ländern Mittel-, Ost- und Südosteuropas ist die Priesterausbildung von entscheidender Bedeutung.

Das Ergebnis der Kollekte ist innerhalb von 14 Tagen mit dem Vermerk „Allerseelen-Kollekte 2016“ auf das Konto der Kirchengemeinde einzuzahlen.

Eine Weiterleitung auf das Konto der Bistumskasse wird durch die jeweils zuständige Rendantur veranlasst. Von dort erfolgt die Abführung an die Aktion Renovabis.

Nähere Informationen zum Allerseelentag sind erhältlich über die Solidaritätsaktion Renovabis, Kardinal-Döpfner-Haus, Domberg 27, 85354 Freising, Telefon (0 81 61) 53 09-53, Telefax (0 81 61) 53 09-44, E-Mail: info@renovabis.de, Internet: www.renovabis.de