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

Vom 5. Oktober 2015

(Kirchliches Amtsblatt Erzbistum Hamburg, 21. Jg., Nr. 10, Art. 128, S. 151 ff.,
v. 20. Oktober 2015)

- Amtliche Lesefassung -

Hiermit erlasse ich zur Umsetzung von Ziffer IV. Anlage 2 zu § 6 KDO der Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO) im Erzbistum Hamburg folgende IT-Richtlinien:

**Präambel**

Die IT-Richtlinien definieren einen Mindeststandard im Rahmen des kirchlichen Datenschutzes. 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, insbesondere auf Buchhaltungsdaten (= DSK II) und Kirchensteuerdaten (= DSK III).

**1. Gemäß 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 Ziffer IV. Anlage 2 zu § 6 KDO Punkt 4.1 bis 4.3). Die jeweils erforderlichen Maßnahmen sind auch bei Auftragsdatenverarbeitung einzuhalten; die Kontrollierbarkeit der Durchführung der Maßnahmen durch den Auftraggeber ist sicher zu stellen.

**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.
- 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 weiter zu geben, 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 mindestens 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 bereit gestellten 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 Ausdrucke 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 gesicherten 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 insbesondere 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) im Erzbistum Hamburg gespeichert (z. B. Public Cloud), sind die Auftragnehmer auf die KDO zu verpflichten. Ergänzend ist sicher zu stellen, dass der physikalische Speicherort der Daten ausschließlich im Geltungsbereich des Bundesdatenschutzgesetzes (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 oder 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, Außerkrafttreten**

Diese IT-Richtlinien treten mit Wirkung zum 1. November 2015 in Kraft. Gleichzeitig tritt die bislang für das Erzbistum Hamburg noch fortgeltende Richtlinie zum Einsatz von Arbeitsplatzcomputern in der Diözese Osnabrück vom 27. Juli 1994 für das Erzbistum Hamburg außer Kraft.

Hamburg, den 5. Oktober 2015

L. S.

Ansgar Thim
- Generalvikar -