

**Beschlüsse der Rechtskommission
des VDD vom 19.03.2015
zur KDO-DVO**

Anlagen 1, 2 und 3

Anlage 1

Durchführungsverordnung

zur Anordnung über den kirchlichen Datenschutz (KDO-DVO)

Die Durchführungsverordnung zur Anordnung über den kirchlichen Datenschutz (KDO-DVO) wird wie folgt geändert:

1. Im Einleitungssatz wird „§ 19 der Anordnung über den kirchlichen Datenschutz (KDO)“ durch „§ 22 der Anordnung über den kirchlichen Datenschutz (KDO)“ ersetzt.
2. Unter Ziffer IV. wird die Überschrift „Anlage zu § 6 KDO“ ersetzt durch „Anlage 1 zu § 6 KDO“.
3. Zu Ziffer IV. wird eine neue Anlage 2 mit folgendem Wortlaut erlassen:

Anlage 2

1.0 Aufgaben und Ziele dieser Anlage

Diese Anlage regelt den Einsatz von Arbeitsplatzcomputern in kirchlichen Stellen. Sie ist als Ergänzung zu § 6 der Anordnung über den Kirchlichen Datenschutz (KDO) und den zu ihr ergangenen bereichsspezifischen Datenschutzregelungen in ihren jeweils geltenden Fassungen anzusehen.

2.0 Arbeitsplatzcomputer/Datenverarbeitungsanlage

- Arbeitsplatzcomputer (APC) im Sinne dieser DVO sind alle selbständigen Systeme der Datenverarbeitung, die von einer kirchlichen Stelle im Sinne des § 1 Abs. 2 KDO zur Erfüllung ihrer Aufgaben genutzt werden.
- Sie können als Einzelgerät (Stand-Alone-PC) oder in Verbindung mit anderen APC (Netzwerken) bzw. anderen Systemen als Datenverarbeitungsanlage installiert sein.
- Als APC sind z.B. auch tragbare Geräte (Laptops bzw. Notebooks oder Netbooks), Tabletcomputer und Mobiltelefone sowie Drucker bzw. Kopierer mit eigener Speichereinheit zu behandeln.

3.0 Allgemeine Grundsätze

3.1 Verantwortlichkeit der Mitarbeiter

- Mitarbeiter im Sinne dieser Anlage sind über die in § 2 Abs. 12 KDO genannten Beschäftigten hinaus auch ehrenamtlich für kirchliche Stellen tätige Personen, die APC verwenden.
- Jeder Mitarbeiter trägt die datenschutzrechtliche Verantwortung für eine vorschriftsmäßige Ausübung seiner Tätigkeit. Es ist ihm untersagt, personenbezogene Daten zu einem anderen als dem in der jeweils rechtmäßigen Aufgabenerfüllung liegenden Zweck zu verarbeiten oder zu übermitteln.

3.2 Verantwortlichkeit der Dienststellenleiter

- Die jeweils als Dienststellenleiter verantwortliche Person ist durch den Generalvikar oder durch die sonst vorgesetzte Dienststelle zu bestimmen.
- Der Dienststellenleiter legt fest, welche im Sinne der KDO schutzwürdigen Daten auf Datenverarbeitungsanlagen gespeichert und verarbeitet werden.
- Ihm obliegt die zutreffende Einordnung der jeweiligen Daten in die Datenschutzklassen nach diesen Richtlinien.

- Der Dienststellenleiter klärt die Mitarbeiter über die Gefahren, die aus der Nutzung einer Datenverarbeitungsanlage erwachsen, sowie über den möglichen Schaden, der kirchlichen Einrichtungen aus einer Datenschutzverletzung erwachsen kann, auf.
- Der Dienststellenleiter stellt sicher, dass ein Konzept zur datenschutzrechtlichen Ausgestaltung der Datenverarbeitungsanlagen erstellt wird.
- Der Dienststellenleiter kann seine Aufgaben und Befugnisse nach dieser Durchführungsverordnung durch schriftliche Anordnung auf geeignete Mitarbeiter übertragen.

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 Daten verarbeitende Stelle die nach der Anlage zu § 6 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:

- Das nach § 3a Abs. 4 KDO zu führende Verzeichnis hat darüber hinaus den regelmäßigen Nutzer, den Standort und die interne Kennzeichnungs-Nummer zu enthalten.
- Alle bei der Verarbeitung personenbezogener Daten beteiligten Personen haben die Verpflichtungserklärung gemäß § 4 Abs. 2 Satz 1 KDO abzugeben. Den Mitarbeitern, die die Verpflichtungserklärung unterschrieben haben, sind die jeweils gültige Anordnung über den Kirchlichen Datenschutz, etwaige Verordnungen, Dienstanordnungen oder Dienstvereinbarungen und die in ihrem Arbeitsbereich zu beachtenden bereichsspezifischen Datenschutzregelungen (Schulen, Krankenhäuser, Friedhöfe etc.) in geschäftsüblicher Weise zugänglich zu machen.
- 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.
- Werden Daten aus den Melderegistern der kommunalen Meldebehörden in kirchlichen Rechenzentren verarbeitet, so orientieren sich die Schutzmaßnahmen an den BSI-IT-Grundschutzkatalogen. Rechenzentren im Sinne dieser Vorschrift sind die für den Betrieb von größeren, zentral in mehreren Dienststellen eingesetzten Informations- und Kommunikationssystemen erforderlichen Einrichtungen.

4.0 Datenschutzklassen

- Das Ausmaß der möglichen Gefährdung personenbezogener Daten bestimmt Art und Umfang der Sicherungsmaßnahmen. Zur Erleichterung der Einordnung bedient sich diese Anlage der Definition dreier Datenschutzklassen, die sich aus der Art der zu verarbeitenden Daten ergeben. Dem Dienststellenleiter, der die Einordnung vornimmt, steht es frei, aus Gründen des Einzelfalles die zu verarbeitenden Daten anders einzuordnen als hier vorgesehen. Diese Gründe sollen kurz dokumentiert werden.
- Bei der Einordnung in die einzelnen Datenschutzklassen ist auf die Daten abzustellen, die vom Benutzer bewusst bearbeitet und gespeichert werden.

4.1 Datenschutzklasse I

Zur Datenschutzklasse I gehören personenbezogene Daten, deren Missbrauch keine besonders schwer wiegende Beeinträchtigung des Betroffenen erwarten lässt. Hierzu

gehören insbesondere Adressangaben ohne Sperrvermerke, z. B. Berufs-, Branchen- oder Geschäftsbezeichnungen.

4.2 Datenschutzklasse II

Zur Datenschutzklasse II gehören personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann. Hierzu gehören z.B. Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und Jubiläumsdaten, usw.

4.3 Datenschutzklasse III

Zur Datenschutzklasse III gehören personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann. Hierzu gehören z.B. Daten über kirchliche Amtshandlungen, gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen, die Mitgliedschaft in einer Religionsgesellschaft, arbeitsrechtliche Rechtsverhältnisse, Disziplinarentscheidungen, usw. sowie Adressangaben mit Sperrvermerken.

4.4 Nicht elektronisch zu verarbeitende 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 oder Verlautbarung würde dem Vertrauen in die Verschwiegenheit katholischer Dienststellen und Einrichtungen schweren Schaden zufügen. Daher dürfen diese Daten nicht auf APC verarbeitet werden, es sei denn, es handelte sich um aus dem staatlichen Bereich übernommene Daten.

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.
- Die Einordnung spricht der Dienststellenleiter aus; er soll einen etwa bestellten betrieblichen Datenschutzbeauftragten und kann den Diözesandatenschutzbeauftragten dazu anhören.
- Wenn keine Einordnung festgelegt ist, gilt automatisch die Datenschutzklasse III, sofern nicht die Voraussetzungen der Ziffer 4.4 vorliegen.

5.0 Besondere Gefahrenlagen

5.1 Nutzung privater Datenverarbeitungssysteme zu dienstlichen Zwecken

Die Verarbeitung personenbezogener Daten auf privaten Datenverarbeitungssystemen zu dienstlichen Zwecken ist grundsätzlich unzulässig. Unter bestimmten Voraussetzungen kann sie als Ausnahme vom Dienststellenleiter genehmigt werden. Die Genehmigung erfolgt schriftlich unter Nennung der Gründe.

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.

Anlage 2

Durchführungsverordnung

zur Anordnung über den kirchlichen Datenschutz (KDO-DVO)

Aufgrund des § 22 der Anordnung über den kirchlichen Datenschutz (KDO) vom 13. Februar 2014 (ABl. 03/2014, Nr. 52, S. 26, Anlage) werden mit Wirkung vom 1. August 2015 die folgenden Regelungen getroffen:

IV. Zu § 6 KDO

Anlage 1

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.

Anlage 2

1.0 Aufgaben und Ziele dieser Anlage

Diese Anlage regelt den Einsatz von Arbeitsplatzcomputern in kirchlichen Stellen. Sie ist als Ergänzung zu § 6 der Anordnung über den Kirchlichen Datenschutz (KDO) und den zu ihr ergangenen bereichsspezifischen Datenschutzregelungen in ihren jeweils geltenden Fassungen anzusehen.

2.0 Arbeitsplatzcomputer/Datenverarbeitungsanlage

- Arbeitsplatzcomputer (APC) im Sinne dieser DVO sind alle selbständigen Systeme der Datenverarbeitung, die von einer kirchlichen Stelle im Sinne des § 1 Abs. 2 KDO zur Erfüllung ihrer Aufgaben genutzt werden.
- Sie können als Einzelgerät (Stand-Alone-PC) oder in Verbindung mit anderen APC (Netzwerken) bzw. anderen Systemen als Datenverarbeitungsanlage installiert sein.
- Als APC sind z.B. auch tragbare Geräte (Laptops bzw. Notebooks oder Netbooks), Tabletcomputer und Mobiltelefone sowie Drucker bzw. Kopierer mit eigener Speichereinheit zu behandeln.

3.0 Allgemeine Grundsätze

3.1 Verantwortlichkeit der Mitarbeiter

- Mitarbeiter im Sinne dieser Anlage sind über die in § 2 Abs. 12 KDO genannten Beschäftigten hinaus auch ehrenamtlich für kirchliche Stellen tätige Personen, die APC verwenden.
- Jeder Mitarbeiter trägt die datenschutzrechtliche Verantwortung für eine vorschriftsmäßige Ausübung seiner Tätigkeit. Es ist ihm untersagt, personenbezogene Daten zu einem anderen als dem in der jeweils rechtmäßigen Aufgabenerfüllung liegenden Zweck zu verarbeiten oder zu übermitteln.

3.2 Verantwortlichkeit der Dienststellenleiter

- Die jeweils als Dienststellenleiter verantwortliche Person ist durch den Generalvikar oder durch die sonst vorgesetzte Dienststelle zu bestimmen.
- Der Dienststellenleiter legt fest, welche im Sinne der KDO schutzwürdigen Daten auf Datenverarbeitungsanlagen gespeichert und verarbeitet werden.
- Ihm obliegt die zutreffende Einordnung der jeweiligen Daten in die Datenschutzklassen nach diesen Richtlinien.
- Der Dienststellenleiter klärt die Mitarbeiter über die Gefahren, die aus der Nutzung einer Datenverarbeitungsanlage erwachsen, sowie über den möglichen Schaden, der kirchlichen Einrichtungen aus einer Datenschutzverletzung erwachsen kann, auf.
- Der Dienststellenleiter stellt sicher, dass ein Konzept zur datenschutzrechtlichen Ausgestaltung der Datenverarbeitungsanlagen erstellt wird.
- Der Dienststellenleiter kann seine Aufgaben und Befugnisse nach dieser Durchführungsverordnung durch schriftliche Anordnung auf geeignete Mitarbeiter übertragen.

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 Daten verarbeitende Stelle die nach der Anlage zu § 6 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:

- Das nach § 3a Abs. 4 KDO zu führende Verzeichnis hat darüber hinaus den regelmäßigen Nutzer, den Standort und die interne Kennzeichnungs-Nummer zu enthalten.
- Alle bei der Verarbeitung personenbezogener Daten beteiligten Personen haben die Verpflichtungserklärung gemäß § 4 Abs. 2 Satz 1 KDO abzugeben. Den Mitarbeitern, die die Verpflichtungserklärung unterschrieben haben, sind die jeweils gültige Anordnung über den Kirchlichen Datenschutz, etwaige Verordnungen, Dienstanordnungen oder Dienstvereinbarungen und die in ihrem Arbeitsbereich zu beachtenden bereichsspezifischen Datenschutzregelungen (Schulen, Krankenhäuser, Friedhöfe etc.) in geschäftsüblicher Weise zugänglich zu machen.
- 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.
- Werden Daten aus den Melderegistern der kommunalen Meldebehörden in kirchlichen Rechenzentren verarbeitet, so orientieren sich die Schutzmaßnahmen an den BSI-IT-Grundschutzkatalogen. Rechenzentren im Sinne dieser Vorschrift sind die für den Betrieb von größeren, zentral in mehreren Dienststellen eingesetzten Informations- und Kommunikationssystemen erforderlichen Einrichtungen.

4.0 Datenschutzklassen

- Das Ausmaß der möglichen Gefährdung personenbezogener Daten bestimmt Art und Umfang der Sicherungsmaßnahmen. Zur Erleichterung der Einordnung bedient sich diese Anlage der Definition dreier Datenschutzklassen, die sich aus der Art der zu verarbeitenden Daten ergeben. Dem Dienststellenleiter, der die Einordnung vornimmt, steht es frei, aus Gründen des Einzelfalles die zu verarbeitenden Daten anders einzuordnen als hier vorgesehen. Diese Gründe sollen kurz dokumentiert werden.
- Bei der Einordnung in die einzelnen Datenschutzklassen ist auf die Daten abzustellen, die vom Benutzer bewusst bearbeitet und gespeichert werden.

4.1 Datenschutzklasse I

Zur Datenschutzklasse I gehören personenbezogene Daten, deren Missbrauch keine besonders schwer wiegende Beeinträchtigung des Betroffenen erwarten lässt. Hierzu gehören insbesondere Adressangaben ohne Sperrvermerke, z. B. Berufs-, Branchen- oder Geschäftsbezeichnungen.

4.2 Datenschutzklasse II

Zur Datenschutzklasse II gehören personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann. Hierzu gehören z.B. Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und Jubiläumsdaten, usw.

4.3 Datenschutzklasse III

Zur Datenschutzklasse III gehören personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann. Hierzu gehören z.B. Daten über kirchliche Amtshandlungen, gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen, die Mitgliedschaft in einer Religionsgesellschaft, arbeitsrechtliche Rechtsverhältnisse, Disziplinarentscheidungen, usw. sowie Adressangaben mit Sperrvermerken.

4.4 Nicht elektronisch zu verarbeitende 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 oder Verlautbarung würde dem Vertrauen in die Verschwiegenheit katholischer Dienststellen und Einrichtungen schweren Schaden zufügen. Daher dürfen diese Daten nicht auf APC verarbeitet werden, es sei denn, es handelte sich um aus dem staatlichen Bereich übernommene Daten.

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.
- Die Einordnung spricht der Dienststellenleiter aus; er soll einen etwa bestellten betrieblichen Datenschutzbeauftragten und kann den Diözesandatenschutzbeauftragten dazu anhören.
- Wenn keine Einordnung festgelegt ist, gilt automatisch die Datenschutzklasse III, sofern nicht die Voraussetzungen der Ziffer 4.4 vorliegen.

5.0 Besondere Gefahrenlagen

5.1 Nutzung privater Datenverarbeitungssysteme zu dienstlichen Zwecken

Die Verarbeitung personenbezogener Daten auf privaten Datenverarbeitungssystemen zu dienstlichen Zwecken ist grundsätzlich unzulässig. Unter bestimmten Voraussetzungen kann sie als Ausnahme vom Dienststellenleiter genehmigt werden. Die Genehmigung erfolgt schriftlich unter Nennung der Gründe.

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.

Anlage 3

IT-Richtlinien zur Umsetzung von IV. Anlage 2 zu § 6 KDO der Durchführungsverordnung zur 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 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 z.B. bei verschlüsselten Daten die Sicherheit des Schlüssels und die erforderliche Entschlüsselung auch im Datensicherungskonzept berücksichtigt werden.

Anm.: 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 sicher zu stellen, 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 Fremdundnehmens auf Datenträgern mit Daten der DSK III sollte nur in besonderen Ausnahmefällen erfolgen. Das Fremdundnehmen 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.

