Schwestern der heiligen
Maria Magdalena Postel

Verordnung
zur Durchführung der Anordnung über den kirchlichen Datenschutz
in der Ordensgemeinschaft der Schwestern der heiligen Maria Magdalena Postel
(KDO-DVO SMMP)

Neufassung gemäß Beschluss der DOK-Mitgliederversammlung vom 15.6.2016

und Beschluss der Leitungsverantwortlichen der Ordensgemeinschaft

der Schwestern der heiligen Maria Magdalena Postel,

vertreten durch die Provinzoberin Sr. Johanna Guthoff vom 01.11.2016

Schwestern der heiligen
Maria Magdalena Postel

Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz

in der Ordensgemeinschaft der Schwestern der heiligen Maria Magdalena Postel
(KDO-DVO SMMP)

Neufassung gemäß Beschluss der DOK-Mitgliederversammlung vom 15.06.2016 und Beschluss der Leitungsverantwortlichen der Ordensgemeinschaft der Schwestern der heiligen Maria Magdalena Postel, vertreten durch die Provinzoberin Sr. Johanna Guthoff vom 01.11.2016

Aufgrund des § 22 der Anordnung über den kirchlichen Datenschutz (KDO SMMP) vom 24.06.2014 werden mit Wirkung vom 01.11.2016 die folgenden Regelungen getroffen:

I. Zu § 3a KDO SMMP (Meldung von Verfahren automatisierter Verarbeitung)

(1) Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind diese vor Inbetriebnahme schriftlich dem Ordensdatenschutzbeauftragten zu melden. Sofern ein betrieblicher Datenschutzbeauftragter bestellt ist, ist diesem gemäß § 21 Absatz 2 KDO SMMP eine Übersicht nach § 3a Absatz 2 KDO SMMP zur Verfügung zu stellen.

(2) Für die Meldung von Verfahren automatisierter Verarbeitung vor Inbetriebnahme beziehungsweise die dem betrieblichen Datenschutzbeauftragten zur Verfügung zu stellende Übersicht soll das Muster gemäß der Anlage zu dieser Verordnung verwandt werden.

II. Zu § 4 KDO SMMP

(1) Zum Kreis der bei der Datenverarbeitung tätigen Personen im Sinne des § 4 KDO SMMP gehören die in den Stellen gemäß § 1 Absatz 2 KDO SMMP gegen Entgelt beschäftigten und ehrenamtlich tätigen Personen sowie dort tätige Ordensangehörige. Sie werden belehrt über:

1. den Inhalt der KDO SMMP und anderer für ihre Tätigkeit geltender Datenschutzvorschriften; dies geschieht durch Hinweis auf die für den Aufgabenbereich des Mitarbeiters wesentlichen Grundsätze und im Übrigen auf die Texte in der jeweils gültigen Fassung. Diese Texte werden zur Einsichtnahme und etwaigen kurzfristigen Ausleihe bereitgehalten; dies wird dem Mitarbeiter bekannt gegeben,
2. die Verpflichtung zur Beachtung der in Nummer 1 genannten Vorschriften bei ihrer Tätigkeit in der Datenverarbeitung,
3. mögliche disziplinarrechtliche bzw. arbeitsrechtliche/rechtliche Folgen eines Verstoßes gegen die KDO SMMP und andere für ihre Tätigkeit geltende Datenschutzvorschriften,
4. das Fortbestehen des Datengeheimnisses nach Beendigung der Tätigkeit bei der Datenverarbeitung.

(2) Über die Beachtung der Verpflichtung ist von den bei der Datenverarbeitung tätigen Personen eine schriftliche Erklärung nach näherer Maßgabe des Abschnittes III abzugeben. Die Urschrift der Verpflichtungserklärung wird zu den Personalakten der bei der Datenverarbeitung tätigen Personen genommen, welche eine Ausfertigung der Erklärung erhalten.

(3) Die Verpflichtung auf das Datengeheimnis erfolgt durch den Dienstvorgesetzten der in der Datenverarbeitung tätigen Personen oder einen von ihm Beauftragten.

III. Zu § 4 Satz 2 KDO SMMP

(1) Die schriftliche Verpflichtungserklärung der bei der Datenverarbeitung tätigen Personen gemäß § 4 Satz 2 KDO SMMP hat zum Inhalt,

1. Angaben zur Identifizierung (Vor- und Zuname, Geburtsdatum und Anschrift sowie Beschäftigungsdienststelle),
2. die Bestätigung, dass auf die für den Aufgabenbereich des Mitarbeiters wesentlichen Grundsätze und im Übrigen auf die Texte in der jeweils gültigen Fassung sowie auf die Möglichkeit der Einsichtnahme und etwaigen kurzfristigen Ausleihe dieser Texte hingewiesen wurde,
3. die Verpflichtung, die KDO SMMP und andere für ihre Tätigkeit geltende Datenschutzvorschriften in der jeweils gültigen Fassung sorgfältig einzuhalten,
4. die Bestätigung, dass sie über disziplinarrechtliche bzw. arbeitsrechtliche Folgen eines Verstoßes gegen die KDO SMMP belehrt wurden.

(2) Die schriftliche Verpflichtungserklärung ist von der bei der Datenverarbeitung tätigen Person unter Angabe des Ortes und des Datums der Unterschriftsleistung zu unterzeichnen.

(3) Für die schriftliche Verpflichtungserklärung ist das Muster gemäß der Anlage zu verwenden.

IV. zu § 6 KDO SMMP

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 SMMP) 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 SMMP 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 SMMP 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 Höheren Oberen oder durch die sonst vorgesetzte Dienststelle zu bestimmen.
- Der Dienststellenleiter legt fest, welche im Sinne der KDO SMMP 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 SMMP 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 SMMP 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 SMMP 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, Seniorenhilfeeinrichtungen 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 anhören und kann den Ordensdatenschutzbeauftragten 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 SMMP. Art und Umfang der Zugriffe sind auf ein Mindestmaß zu reduzieren und gesondert zu regeln. Für die Fernwartung gilt § 8 KDO SMMP entsprechend.

V. Zu § 12 Absatz 3 KDO SMMP

(1) Die Unterrichtung des Betroffenen (§ 2 Absatz 1 KDO SMMP) über eine Übermittlung gemäß § 12 Absatz 3 Satz 1 KDO SMMP erfolgt schriftlich.

(2) Sie enthält

1. die Bezeichnung der übermittelnden Stelle einschließlich der Anschrift,
2. die Bezeichnung des Dritten, an den die Daten übermittelt werden, einschließlich der Anschrift,
3. die Bezeichnung der übermittelten Daten.

VI. Zu § 13 Absatz 1 KDO SMMP

(1) Der Antrag des Betroffenen (§ 2 Absatz 1 KDO SMMP) auf Auskunft ist schriftlich an die verantwortliche Stelle (§ 2 Absatz 8 KDO SMMP) zu richten oder dort zu Protokoll zu erklären.

(2) Der Antrag soll die Art der personenbezogenen Daten, über die Auskunft begehrt wird, näher bezeichnen. Der Antrag auf Auskunft über personenbezogene Daten, die weder automatisiert verarbeitet noch in einer nicht automatisierten Datei gespeichert sind, muss Angaben enthalten, die das Auffinden der Daten ermöglichen.

(3) Der Antrag kann beschränkt werden auf Auskunft über

1. die zur Person des Betroffenen gespeicherten Daten oder
2. die Herkunft dieser Daten oder
3. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben worden sind oder
4. den Zweck, zu dem diese Daten gespeichert sind.

(4) Vorbehaltlich der Regelung in § 13 Absatz 3 KDO SMMP wird die Auskunft in dem beantragten Umfang von der verantwortlichen Stelle (§ 2 Absatz 8 KDO SMMP) schriftlich erteilt.

(5) Wenn die Erteilung der beantragten Auskunft gemäß § 13 Absatz 2 oder 3 KDO SMMP zu unterbleiben hat, so ist dies dem Antragsteller schriftlich mitzuteilen. Die Versagung der beantragten Auskunft soll begründet werden. Für den Fall, dass eine Begründung gemäß § 13 Absatz 4 KDO SMMP nicht erforderlich ist, ist der Antragsteller darauf hinzuweisen, dass er sich an den Ordensdatenschutzbeauftragten wenden kann; die Anschrift des Ordensdatenschutzbeauftragten ist ihm mitzuteilen.

VII. Zu § 13a KDO SMMP

(1) Die Benachrichtigung des Betroffenen (§ 2 Absatz 1 KDO SMMP) gemäß § 13 a Absatz 1 KDO SMMP erfolgt, soweit die Pflicht zur Benachrichtigung nicht nach § 13a Absatz 2 und 3 entfällt, schriftlich durch die verantwortliche Stelle.

(2) Sie enthält

1. die zur Person des Betroffenen gespeicherten Daten,
2. die Bezeichnung der verantwortlichen Stelle,
3. den Zweck, zu dem die Daten erhoben, verarbeitet oder genutzt werden,
4. die Empfänger oder Kategorien von Empfängern, soweit der Betroffene nicht mit der Übermittlung an diese rechnen muss.

VIII. Zu § 14 KDO SMMP

(1) Der Betroffene (§ 2 Absatz 1 KDO SMMP) kann schriftlich beantragen, ihn betreffende personenbezogene Daten zu berichtigen oder zu löschen. Der Antrag ist schriftlich an die Stellen gemäß § 1 Absatz 2 Nr. 2 und 3, im Falle des § 1 Absatz 2 Nr. 1 an die Ordensgemeinschaft / das Kloster zu richten.

(2) In dem Antrag auf Berichtigung sind die Daten zu bezeichnen, deren Unrichtigkeit behauptet wird. Der Antrag muss Angaben über die Umstände enthalten, aus denen sich die Unrichtigkeit der Daten ergibt.

(3) In dem Antrag auf Löschung sind die personenbezogenen Daten zu bezeichnen, deren Speicherung für unzulässig gehalten wird. Der Antrag muss Angaben über die Umstände enthalten, aus denen sich die Unzulässigkeit der Speicherung ergibt.

(4) Die zuständige Stelle entscheidet schriftlich über Anträge gemäß Absatz 1. Die Entscheidung ist dem Antragsteller bekannt zu geben. Im Falle des § 14 Absatz 8 KDO SMMP sind ihm die Stellen anzugeben, die von der Berichtigung, Löschung oder Sperrung verständigt worden sind. Ist eine Verständigung aufgrund des § 14 Absatz 8 KDO SMMP unterblieben, sind dem Antragsteller die Gründe dafür mitzuteilen.

(5) Der Widerspruch gemäß § 14 Absatz 5 KDO SMMP ist schriftlich oder zur Niederschrift bei der verantwortlichen Stelle (§ 2 Absatz 8 KDO SMMP) einzulegen. Die Umstände, aus denen sich das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation ergibt, sind von dem Betroffenen darzulegen. Die verantwortliche Stelle entscheidet über den Widerspruch in geeigneter Form. Die Entscheidung ist dem Betroffenen bekannt zu geben.

Schwestern der heiligen
Maria Magdalena Postel

Anlagen

1. Zu Abschnitt I. KDO-DVO SMMP (§ 3a KDO SMMP Meldung von Verfahren automatisierter Verarbeitungen)

Die Notwendigkeit für die in den nachfolgenden Formularen (Muster 1 und Muster 2) geforderten Angaben ergibt sich aus § 3a KDO SMMP. Für jedes automatisierte Verfahren einer verantwortlichen Stelle füllt der Rechtsträger (§ 1 Absatz. 2 KDO SMMP) ein Formular nach Muster 1 und Muster 2 aus.

Schwestern der heiligen
Maria Magdalena Postel

Muster 1

Allgemeine Angaben (§ 3a Absatz 2 Nr. 1 und Nr. 2 KDO SMMP)
1. Name und Anschrift
1.1 des Rechtsträgers (§ 1 Absatz 2 KDO SMMP) *(z.B. von SMMP getragen€ GmbH oder e.V.)*
1.2 der verantwortlichen Stelle (Jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt [§ 2 Absatz 8 KDO SMMP]) *(z.B. Schule oder Senioreneinrichtung der GmbH)*

2. Vertretung der verantwortlichen Stelle
2.1 der nach der Verfassung (Statut, Geschäftsordnung, Satzung) berufene Leiter der verantwortlichen Stelle *(z.B. Leiterin des Schule oder Senioreneinrichtung der GmbH)*
2.2 mit der Leitung der Datenverarbeitung in der verantwortlichen Stelle beauftragte Personen *(z.B. beauftragte Mitarbeiterin in der Schule oder Senioreneinrichtung)*

Besondere Angaben (§ 3a Absatz 2 Nr. 3 bis Nr. 7 KDO SMMP)
3. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung (z.B. Mitglieder- und Bestandspflege)

4. Betroffene Personengruppen und Daten oder Datenkategorien

4.1 Beschreibung der betroffenen Personengruppen *(z. B. Mitarbeiter, Angehöriger der Schüler oder Bewohner, Schüler oder Bewohner usw.)*

4.2 Beschreibung der diesbezüglichen Daten oder Datenkategorien *(Mit „Daten" sind „personenbezogene Daten" i. S. d. § 2 Absatz 1 KDO SMMP gemeint, wie z.B. Name, Anschrift, Geburtsdatum, Religionszugehörigkeit. Grundsätzlich reicht jedoch die Angabe von Datenkategorien, z.B. Personaldaten, aus. Sogenannte „besondere Arten personenbezogener Daten" (vgl. § 2 Absatz 10 KDO SMMP) sind entsprechend anzugeben.)*

5. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können (Jede Person oder Stelle, die Daten erhält [§ 2 Absatz 9 KDO SMMP]) *(z.B. Behörden, kirchliche Stellen, Versicherungen, ärztliches Personal usw.)*

6. Regelfristen für die Löschung der Daten

7. Geplante Datenübermittlung ins Ausland

_____

Ort, Datum, Unterschrift

Schwestern der heiligen
Maria Magdalena Postel

Muster 2

Allgemeine Angaben (§ 3a Absatz 2 Nr. 1 und Nr. 2 KDO SMMP)

1. Name und Anschrift
1.1 des Rechtsträgers (§ 1 Absatz 2 KDO SMMP) *(z.B. von SMMP getragene® GmbH oder e.V.)*
1.2 der verantwortlichen Stelle (Jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt [§ 2 Absatz 8 KDO SMMP]) *(z.B. Schule oder Senioreneinrichtung der GmbH)*

2. Vertretung der verantwortlichen Stelle
2.1 der nach der Verfassung (Statut, Geschäftsordnung, Satzung) berufene Leiter der verantwortlichen Stelle *(z.B. Leiterin der Schule oder Senioreneinrichtung der GmbH)*
2.2 mit der Leitung der Datenverarbeitung in der verantwortlichen Stelle beauftragte Personen *(z.B. beauftragte Mitarbeiterin in der Schule oder Senioreneinrichtung)*

Besondere Angaben (§ 3a Absatz 2 Nr. 8 und Nr. 9 KDO SMMP)
3. Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (z.B. Konfigurationsübersicht, Netzwerkstruktur, Betriebs- und Anwendungssoftware, spezielle Sicherungssoftware usw.)

4. Zugriffsberechtigte Personen

_____

Ort, Datum, Unterschrift

Schwestern der heiligen
Maria Magdalena Postel

2. Zu Abschnitt III. KDO-DVO SMMP (§ 4 Satz 2 KDO SMMP) :

Verpflichtungserklärung

Ich verpflichte mich,

1. die Anordnung über den kirchlichen Datenschutz der Ordensgemeinschaft der Schwestern der hl. Maria Magdalena Postel (KDO SMMP) in der jeweils geltenden Fassung sowie die anderen für meine Tätigkeit geltenden Datenschutzregelungen einschließlich der zu ihrer Durchführung ergangenen Bestimmungen sorgfältig einzuhalten und bestätige, dass ich auf die wesentlichen Grundsätze der für meine Tätigkeit geltenden Bestimmungen hingewiesen wurde. Ich wurde ferner darauf hingewiesen, dass die KDO SMMP und die Texte der übrigen für meine Tätigkeit geltenden Datenschutzvorschriften bei meiner Einrichtungsleitung eingesehen und auch für kurze Zeit ausgeliehen werden können.
Weitere Informationen zum Datenschutz befinden sich im Internet unter http://www.smmp.de.

2. das Datengeheimnis auch nach Beendigung meiner Tätigkeit zu beachten.

Ich bin darüber belehrt worden, dass ein Verstoß gegen das Datengeheimnis gleichzeitig einen Verstoß gegen die Schweigepflicht darstellt, der disziplinarrechtliche beziehungsweise arbeitsrechtliche/rechtliche Folgen haben kann.

Diese Erklärung wird zu den Akten genommen.

Vor- und Zuname, Anschrift:

_____ _____

Ort, Datum Unterschrift

Schwestern der heiligen
Maria Magdalena Postel

IT-Richtlinien

zur Umsetzung der Durchführungsverordnung zur Anordnung über den kirchlichen Datenschutz (KDO/DVO SMMP) Punkt IV. zu § 6, Anlage 2

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 SMMP IV. Anlage 2 zu § 6 KDO SMMP 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 SMMP) gespeichert (z.B. Public Cloud), sind die Auftragnehmer auf die KDO SMMP 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 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 SMMP 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.