Der Diözesandatenschutzbeauftragte

des Erzbistums Hamburg
der Bistümer Hildesheim, Osnabrück und
des Bischöflich Münsterschen Offizialats in Vechta i.O.

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Mustervertrag
zur Vernichtung von Datenträgern
mit sensiblen personenbezogenen Daten nach DIN 66399

(MV 204 - Stand: 13.10.2014)

Vorbemerkung:

In vielen Bereichen der kirchlichen Arbeit besteht die Notwendigkeit, in gewissen Zeitabständen Akten zu vernichten, da diese nicht mehr für die eigene Arbeit benötigt werden und auch keine Verpflichtung zu ihrer dauerhaften Verwahrung besteht. Eventuelle Aufbewahrungsfristen sind bereits abgelaufen. In der heutigen Zeit sind hiervon jedoch nicht nur Papierdokumente betroffen, sondern auch elektronische Medien, wie CDs, Festplatten oder Speichersticks.

Im Oktober 2012 hat daher das Deutsche Institut für Normung (DIN), unter Beteiligung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine technische Richtlinie herausgegeben, die die Vernichtung aller Datenträger von Papier bis hin zu Chipkarten zum Gegenstand hat. Gleichzeitig wurde die bisherige Empfehlung für den Einsatz von Aktenvernichtern, die DIN 32757-1 zurückgezogen. Angesichts der Vielzahl heute eingesetzter Datenträger wurde sie nicht mehr als ausreichend angesehen. Die neue Normung, die „DIN 66399: Büro und Datentechnik – Vernichtung von Datenträgern“ besteht aus drei Teilen.

1. DIN 66399-1 Grundlagen und Begriffe
2. DIN 66399-2 Anforderungen an Maschinen zur Vernichtung von Datenträgern
3. DIN 66399-3 SPEC Prozesse der Datenträgervernichtung

Die Einhaltung der Norm ist nicht verbindlich. Die Ergebnisse der Arbeit des Deutschen Instituts für Normung haben keine Gesetzesqualität. Insoweit kann man die Norm beachten oder auch anders verfahren. Trotzdem wird **dringend** empfohlen, sich bei der Vernichtung von Datenträgern hieran zu halten. Im Bereich der Datenschutzbeauftragten des Bundes und der Länder ist anerkannt, dass eine Entsorgung nicht mehr benötigter Datenträger unter Beachtung der DIN 66399 als datenschutzgerecht anzusehen ist. Der Mustervertrag setzt die Anforderungen der Norm vollständig um. Er bezieht sich hierbei auf die Vernichtung sehr sensibler Daten, die dem Geheimnisschutz nach § 203 StGB unterliegen. In Fällen, wo diese Voraussetzung nicht vorliegt, sondern eine andere, geringere Schutzklasse der Daten vorliegt, kann das Muster entsprechend den DIN-Vorgaben abgewandelt werden.

Die Anwendung der Norm ist ganz einfach!

In einem ersten Schritt muss entschieden werden, wie hoch der Schutzbedarf für die auf den Datenträgern gespeicherten Informationen ist. Medizinische Daten, Klientendaten aus anerkannten Beratungsstellen, Sozialdaten beispielsweise gehören zur Schutzklasse 3.

Im zweiten Schritt muss dann die anzuwendende Sicherheitsstufe bestimmt werden. Nach der Tabelle sind für Datenträger, die zur Schutzklasse 3 gehören, die Sicherheitsstufen 4 bis 7 anzuwenden. Stufe 4 gibt also die zu verwirklichende Mindestvoraussetzung an. Welche Stufe im Einzelfall angemessen ist, lässt sich aus der Beschreibung der Sicherheitsstufen entnehmen. So ist in Sicherheitsstufe 3 die Reproduktion des Materials nur mit erheblichen Aufwand, in Stufe 4 mit außergewöhnlichem Aufwand und in Stufe 5 nur mit zweifelhaften Methoden möglich. Bei der Stufe 6 ist eine Reproduktion technisch nicht möglich und bei Stufe 7 sogar gänzlich ausgeschlossen. Stufe 4 ist hier als ausreichend anzusehen, die Stufen 6 und 7 sind für Geheimdienstmaterial vorgesehen.

Tabelle: Anwendung der DIN 66399 Teil 1

1. Schritt	**Ermittlung des Schutzbedarfs**		
	Schutzklasse 1 Normaler Bedarf (interne Daten)	**Schutzklasse 2** Hoher Bedarf (vertrauliche Daten)	**Schutzklasse 3** Sehr hoher Bedarf (besonders geheime Daten)
2. Schritt	**Bestimmung der anzuwenden Sicherheitsstufe**		
Stufe 1:	Allgemeine Daten (Reproduktion mit einfachem Aufwand)[1]	nein	nein
Stufe 2:	Interne Daten[2] (Reproduktion mit besonderem Aufwand)	nein	nein
Stufe 3:	Sensible Daten (Reproduktion mit erheblichem Aufwand)	Sensible Daten (Reproduktion mit erheblichem Aufwand)	nein
Stufe 4:	nicht vorgesehen	Besonders sensible Daten (Reproduktion mit außergewöhnlichem Aufwand)	Besonders sensible Daten (Reproduktion mit außergewöhnlichem Aufwand)
Stufe 5:	nicht vorgesehen	Geheim zu haltende Daten (Reproduktion mit zweifelhaften Methoden)	Geheim zu haltende Daten (Reproduktion mit zweifelhaften Methoden)
Stufe 6:	nicht vorgesehen	nicht vorgesehen	Geheime Hochsicherheitsdaten (Reproduktion technisch nicht möglich)
Stufe 7:	nicht vorgesehen	nicht vorgesehen	Top Secret Hochsicherheitsdaten (Reproduktion ausgeschlossen)

[1] Nicht bei personenbezogenen Daten
[2] Nicht bei personenbezogenen Daten

Im dritten Schritt wird nunmehr die bei der Vernichtung einzusetzende Technik bestimmt. Sie kann dem zweiten Teil der DIN-Norm entnommen werden. Hier sind sechs verschiedene Datenträgergruppen benannt. Für jede Gruppe gibt es, entsprechend den Sicherheitsstufen genaue Angaben, wie die Vernichtung durchzuführen ist und welche Partikelgrößen dabei als zulässig angesehen werden. Als Datenträgerarten sind erfasst:

Tabelle: Anwendung der DIN 66399 Teil 2

P	Informationsdarstellung in Originalgröße	Papier, Filme, Druckformen
F	Informationsdarstellung verkleinert	Filme, Mikrofilme, Folien
O	Informationsdarstellung auf optischen Datenträgern	CD, DVD
T	Informationsdarstellung auf magnetischen Datenträgern	Disketten, Magnetbänder, ID-Karten
H	Informationsdarstellung auf Festplatten mit magnetischem Datenträger	Festplatten
E	Informationsdarstellung auf elektronischen Datenträgern	Chipkarten, Speichersticks, Halbleiterfestplatten, mobile Kommunikationsmittel

Das bedeutet, dass Patientendaten, die zur Schutzklasse 3 und der Sicherheitsstufe 4 gehören, nach P-4 zu vernichten sind, wenn es sich um Papierdokumente handelt. Sind die Daten auf einer CD gespeichert, so ist die Vernichtung nach O-4 vorzunehmen und bei einer Festplatte nach H-4.

Der Mustervertrag sieht vor, dass die Datenträger benannt werden und bestimmt wird, nach welcher Norm sie zu vernichten sind. Die Einhaltung dieser Norm ist vom Auftragnehmer nachzuweisen.

Bleibt nur noch, in einem vierten Schritt, das Verfahren zu bestimmen und ordnungsgemäß abzusichern. Vorgaben hierfür sind in DIN 66399-3 benannt. In dem Mustervertrag wurden die hier geregelten Varianten 2 (Datenträgervernichtung durch einen Dienstleister beim Auftraggeber) und 3 (externe Datenträgervernichtung durch Dienstleister) zu Grunde gelegt. **Wichtige** Voraussetzungen nach der Festlegung in DIN 66399-3 hierbei sind:

1. Die Sammlung des Materials in verschlossenen Sicherheitsbehältern
2. Die Erstellung eines Übernahmeprotokolls
3. Der Einsatz von Maschinen zur Vernichtung nach DIN 66399-2
4. Die Erstellung eines Vernichtungsprotokolls
5. Das vorherige Überschreiben und Löschen elektronischer oder magnetischer Datenträger durch den Auftraggeber
6. Verpflichtungserklärung nach § 4 KDO auf das Datengeheimnis der Mitarbeiter

Diese Voraussetzungen wurden in den Mustervertrag aufgenommen. Natürlich sind noch eine Reihe weiterer organisatorischer Maßnahmen zu treffen, die auf Seiten des Auftraggebers (Durchführung der Sammlung, Anfallstelle, Lagerung und Transport) und auf Seiten des Auftragnehmers (Betriebsgebäude, Sicherheitszone, Zugangssperren für unautorisierte Personen)

erfüllt sein müssen. Soweit sie den Auftragnehmer betreffen, sollten sie in einer Darstellung über die Organisation beim Dienstleister als Anlage mit zum Vertrag genommen werden (Anlage 2). Für den Auftraggeber ist weiterhin eine Dienstanweisung für Mitarbeiter erforderlich, wie die Sammlung und Lagerung des zu vernichtenden Materials durchgeführt werden soll.

Hannover, den 13. Oktober 2014

Mustervertrag
zur Vernichtung von Datenträgern
mit sensiblen personenbezogenen Daten nach DIN 66399

Zwischen._____
(im Folgenden Auftraggeber genannt)

und._____
(im Folgenden Auftragnehmer genannt)

wird folgender Vertrag geschlossen:

§ 1 Vertragsgegenstand

(1) Gegenstand des Vertrages ist die Entsorgung und Vernichtung von Datenträgern, unter der Anwendung der DIN-Normen 66399-1, 66399-2 und DIN-SPEC 66399-3.

(2) Die vom Auftraggeber und seinen Mitarbeitern verarbeiteten Daten unterliegen der Geheimhaltungspflicht nach § 203 StGB. Aus diesem Grunde fallen die dem Auftragnehmer zur Vernichtung übergebenen Datenträger in die Schutzklasse 3 (sehr hoher Bedarf für besonders geheime Daten) und sind mindestens nach der Sicherheitsstufe 4 der DIN 66399-1 als besonders sensible Daten zu vernichten. Der Auftragnehmer übernimmt daher die Verpflichtung, diese Datenträger unter strenger Einhaltung der entsprechenden Vernichtungsregeln, entsprechend der DIN 66399-2 zu entsorgen.

(3) Die nachfolgenden Datenträgerarten werden dem Auftragnehmer übergeben[1]:

- ☐ Datenträger P mit einer Informationsdarstellung in Originalgröße (Papier, Film, Druckformen)
- ☐ Datenträger F mit verkleinerter Informationsdarstellung (Film, Mikrofilm, Folie)
- ☐ Datenträger O mit Informationsdarstellung auf optischen Datenträgern (CD, DVD)
- ☐ Datenträger T mit Informationsdarstellung auf magnetischen Datenträgern (Disketten, Magnetbänder, ID-Karten)
- ☐ Datenträger H mit Informationsdarstellung auf Festplatten mit magnetischem Datenträger
- ☐ Datenträger E mit Informationsdarstellung auf elektronischen Datenträgern (Speicherstick, Chipkarten, Halbleiterfestplatten, mobile Kommunikationsmittel)

(4) Die Vernichtung dieser Datenträger wird mit Maschinen nach den in der DIN 66399-2 festgelegten Standards P-4, F-4, O-4, T-4, H-4 und E-4 vorgenommen. Der Auftragnehmer ist verpflichtet dem Auftraggeber hierüber einen geeigneten Nachweis zu erbringen.

[1] Zutreffendes ankreuzen

§ 2 Entsorgungsverfahren

(1) Der Auftraggeber wird die anfallenden Datenträger getrennt, nach der zu erreichenden Sicherheitsstufe und der von ihm vorzunehmenden Einstufung der Schutzklasse sortieren. Elektronische und magnetische Datenträger sind dabei nach Möglichkeit vorab zu löschen und zu überschreiben.

(2) Die Datenträger werden in folgenden Schutzbehältern der Firma …… bis zur Abholung durch den Auftragnehmer sicher verwahrt.

(3)[2] Der Auftragnehmer holt die Datenträger mit einem geschlossenen Spezialfahrzeug bzw. Spezialcontainer innerhalb von ... Stunden nach Anforderung / spätestens am zweiten Arbeitstag nach Anforderung des Auftraggebers ab. Die Übergabe erfolgt erst nach Ausfertigung eines Protokolls, in dem mindestens folgende Angaben festzuhalten sind:

- der Name des Boten,
- die Sicherheitseinstufung der übergebenen Datenträger,
- die Menge der Behälter je Datenträgertyp und
- der Zeitpunkt und Ort der Übergabe.

Der Auftragnehmer garantiert, dass das zu vernichtende Material während des Transportes nicht verloren geht oder entnommen werden kann.

(4) Der Auftragnehmer haftet ab dem Zeitpunkt der Übernahme für das zu vernichtende Material. Er stellt durch geeignete technische und organisatorische Maßnahmen sicher, dass zwischen Übernahme und Abschluss der Vernichtung unberechtigte Dritte keinen Zugang zu dem Material haben.

(5) Die Vernichtung wird im Betrieb des Auftragnehmers durchgeführt. Dabei wird ein Vernichtungsprotokoll erstellt, das mindestens folgende Angaben enthält:

- den Namen der Person, die die Vernichtung durchgeführt hat
- Uhrzeit und Ort der Vornahme sowie
- Angaben zur Sicherheitsstufe nach DIN 66399-2
- besondere Vorkommnisse, Störungen des Betriebes
- Unterschrift eines befugten Mitarbeiters des Auftragnehmers

Eine Ausfertigung des Protokolls ist dem Auftraggeber zuzuleiten.

(5)[3] Der Auftragnehmer wird die Entsorgung der Datenträger im Bereich der Betriebsstätte des Auftraggebers durchführen. Hierzu wird er zum jeweils vereinbarten Zeitpunkt ein Spezialfahrzeug, das die nach DIN 66399-2 erforderlichen Maschinen für die vom Auftraggeber angegebene Sicherheitsstufe enthält, zum Auftraggeber entsenden.

(6) Die Übernahme des Materials erfolgt nach Ausstellung eines Protokolls, das folgende Angaben enthält:

---

[2] Alternativlösung 1: Die Datenträgervernichtung erfolgt extern durch den Auftragnehmer. Bei dieser Lösung sind die grün gefärbten Absätze zu streichen.

[3] Alternativlösung 2: Die Datenträgervernichtung erfolgt vor Ort durch den Auftragnehmer. Bei dieser Lösung sind die blau gefärbten Absätze zu streichen.

- der Name des Boten,

- die Sicherheitseinstufung der übergebenen Datenträger,

- die Menge der Behälter und

- der Zeitpunkt und Ort der Übergabe.

Die Übergabe erfolgt durch einen vom Auftraggeber benannten Mitarbeiter. Ihm wird eine Ausfertigung des Übernahmeprotokolls übergeben.

(7) Die Vernichtung der übergebenen Datenträger erfolgt anschließend, unter Beisein des Mitarbeiters des Auftraggebers mit den Maschinen des Spezialfahrzeugs. Anschließend wird ein Vernichtungsprotokoll erstellt und übergeben, das die folgenden Angaben enthält:

- den Namen der Person, die die Vernichtung durchgeführt hat

- Uhrzeit und Ort der Durchführung sowie

- Angaben zur durchgeführten Sicherheitsstufe nach DIN 66399-2

- besondere Vorkommnisse, Störungen des Betriebes

- Unterschrift des Mitarbeiters des Auftragnehmers

(8) Die Entsorgungslogistik (Bereitstellung von verschließbaren Behältern bzw. Containern auf Mietbasis) wird zwischen den Vertragspartnern auf Grundlage der Anlage 1 zu diesem Vertrag schriftlich vereinbart. Im Falle der externen Datenträgervernichtung gewährleistet der Auftragnehmer, dass die Datenträger während des Transportes nicht mit den Datenträgern anderer Auftraggeber vermischt werden.

§ 3 Rechte am Material

(1) Der Auftragnehmer erwirbt keine Rechte an dem in seinen Besitz gelangenden Material und den darauf verzeichneten Daten, schriftlichen oder bildlichen Darstellungen. Die Einsichtnahme in das Material sowie dessen Weitergabe oder sonstige Verwendung durch den Auftragnehmer - auch in immaterieller Form - ist untersagt.

(2) Der Auftraggeber ist jedoch damit einverstanden, dass das vernichtete Material zum Zwecke der Entsorgung an entsprechende Dienstleister verkauft wird.

§ 4 Datenschutz

(1) Der Auftragnehmer beachtet bei der Entsorgung und Vernichtung der Datenträger die datenschutzrechtlichen Bestimmungen der KDO und des BDSG. Er unterwirft sich den Bestimmungen der Aufsicht des Diözesandatenschutzbeauftragten des (Erz-) Bistums _____ gemäß §§ 18,19 der Anordnung über den kirchlichen Datenschutz - KDO in der jeweils geltenden Fassung.

(2) Der Auftragnehmer verpflichtet sich, die Vorschriften der KDO, insbesondere die §§ 4 und 6 einzuhalten und die gemäß der Anlage zu § 6 getroffenen Maßnahmen in einer Aufstellung (Anlage 2) zu diesem Vertrag zu dokumentieren.

(3) Der Auftragnehmer verpflichtet seine bei der Entsorgung und Vernichtung der Datenträger eingesetzten Mitarbeiter schriftlich auf das Datengeheimnis gemäß § 4 KDO und

kontrolliert die Einhaltung der datenschutzrechtlichen Bestimmungen. Darüber hinaus sind alle Mitarbeiter des Auftragnehmers auf die Einhaltung der Bestimmungen des Strafgesetzbuches (§§ 203, 204 StGB) hinzuweisen und entsprechend zu belehren. Dies ist schriftlich nachzuweisen.

§ 5 Weitere Pflichten der Vertragsparteien

(1) Der Auftragnehmer ist nicht berechtigt, ohne vorherige Absprache mit dem Auftraggeber, ein anderes Unternehmen mit dem Abtransport der Behälter/Container zu beauftragen.

(2) Der Auftragnehmer ist berechtigt / nicht berechtigt, Unteraufträge zur Vernichtung der Datenträger zu erteilen. Im Falle der Berechtigung hat der Auftragnehmer den Sub-Auftragnehmer zur Einhaltung dieser Regelungen und der datenschutzrechtlichen Bestimmungen vertraglich zu verpflichten. Der Auftragnehmer kontrolliert die Einhaltung dieser Pflichten bei dem Sub-Unternehmer. Der Auftraggeber ist über den Einsatz von Sub-Auftragnehmern zu informieren.

(3) Im Falle außergewöhnlicher innerbetrieblicher Vorkommnisse (z. B. Unfälle, Krankheiten) ist der Auftragnehmer berechtigt, einen bereits bestätigten Termin der Auftragserfüllung in Absprache mit dem Auftraggeber zu verschieben.

(4) Der Auftragnehmer gewährleistet, dass bei gemeinschaftlicher Vernichtung von Datenträgern mehrerer Auftraggeber die jeweils anderen Auftraggeber keine Kenntnis der auf den Datenträgern gespeicherten Daten erhalten, und dass die Vertraulichkeit der Daten durch die Ausübung der Kontroll- oder Eigentumsrechte anderer Auftraggeber nicht beeinträchtigt wird.

(5) Die Beladung des Spezialfahrzeuges bzw. Spezialcontainers erfolgt durch den Auftraggeber oder unter Aufsicht des Auftraggebers durch Arbeitskräfte des Auftragnehmers auf Grundlage einer zusätzlichen Berechnung dieser Leistung.

(6) Die Anlieferung/Abholung des zu vernichtenden Materials ist zwischen den Vertragspartnern terminlich abzustimmen. Die zu entsorgenden Datenträger sind am selben Tag zu vernichten.

(7) Die Vernichtung erfolgt an folgendem Ort: _____

(8) Der Auftraggeber hat das Recht, Transport und Vernichtung des Materials durch einen eigenen Mitarbeiter begleitend oder nachträglich kontrollieren zu lassen.

(9) Als Ansprechpartner des Auftragnehmers wird benannt:

_____

Als Ansprechpartner des Auftraggebers wird benannt:

_____

§ 6 Entgelte

(1) Für die Entsorgung hat der Auftraggeber folgendes Entgelt an den Auftragnehmer zu entrichten:

…..

(2) Alle Entsorgungs- und Transportkosten verstehen sich zuzüglich der zurzeit gültigen Mehrwertsteuer.

(3) Die Entgelte basieren auf der derzeitigen Marktlage für Wertstoffe, den derzeitigen Deponiekosten, dem Index für Investitionskosten, dem Güternahverkehrstarif, den Tarifvereinbarungen, den Kosten für die Aufbereitung von Wertstoffen, den Transportkosten, dem Index für Mineralölerzeugnisse und dem Index für Straßenfahrzeuge.

(4) Ändern sich Kostenbestandteile, so sind die daraus resultierenden Entgelte neu zu kalkulieren und neu zu vereinbaren. Die Änderung des Vertrages tritt einen Monat nach der Vereinbarung in Kraft.

§ 7 Haftung

(1) Der Auftragnehmer haftet dem Auftraggeber für Transport und Vernichtung des Materials nach diesem Vertrag sowie den gesetzlichen Bestimmungen.

(2) Der Auftragnehmer hält den Auftraggeber insbesondere von solchen Ansprüchen Dritter frei, die gegen den Auftraggeber erhoben werden und die durch nicht vertragsgemäße Behandlung des Materials nach Übernahme durch den Auftragnehmer begründet sind.

(3) Der Auftragnehmer haftet nicht für den Fall, dass der Auftraggeber ihm irrtümlich falsches Material zur Vernichtung übergeben hat.

(4) Die Vernichtung der Daten geschieht in einem gesondert gesicherten Betriebsbereich.

(5) Bei Verdacht auf Verletzungen des Datenschutzes und bei anderen Unregelmäßigkeiten (z.B. Transportunfällen) wird der Auftraggeber unverzüglich benachrichtigt.

§ 8 Vertragsdauer

(1) Der Vertrag beginnt am: _____

(2) Der Vertrag wird auf unbestimmte Dauer geschlossen und kann jederzeit, jedoch erstmals zum Ablauf des ersten Kalenderjahres, mit einer Frist von drei Monaten zum Monatsende gekündigt werden.

(3) Für jeden Fall der Zuwiderhandlung gegen die sich aus §§ 4 und 5 ergebenden Pflichten des Auftragnehmers, insbesondere für den Fall einer Zuwiderhandlung gegen datenschutzrechtliche Bestimmungen, steht dem Auftraggeber das Recht der fristlosen Kündigung zu.

§ 9 Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, so zum Beispiel durch eine Pfändung oder Beschlagnahme, durch Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(2) Jede Änderung und Ergänzung dieses Vertrages hat schriftlich zu erfolgen. Mündliche Absprachen haben keine rechtsverbindliche Gültigkeit.

(3) Sollten einzelne Bestimmungen des Vertrages unvollständig sein oder werden, so wird dadurch die Gültigkeit der übrigen Vereinbarungen nicht berührt. Im Falle einer unvollständigen Regelung soll die Lücke durch Auslegung des im übrigen Vertragstext niedergelegten Parteiwillens derart geschlossen werden, wie dies dem wirtschaftlichen Ziel des Vertrages am ehesten entspricht.

(4) Gerichtsstand ist: _____

Anlage 1

gemäß § 2 Absatz VIII des Vertrages

Vereinbarung über zu mietende Behälter/Container

Monatliche Mietkosten pro Stück:

..... Stück Absetzcontainer, 10 m³, geschlossen mit Deckel

..... Stück Absetzcontainer, 10 m³, geschlossen mit Türen

..... Stück Umleerbehälter, 1,1 m³

..... Stück Kunststofftonnen, 240 Liter Inhalt

Alle Behälter/Container sind verschließbar und vor dem Zugriff Unbefugter geschützt

Anlage 2

gemäß § 4 Absatz 2 des Vertrages[4]

Zum Schutz der Daten, die der Auftragnehmer im Rahmen dieses Vertrages für den Auftraggeber vernichtet sind beim Auftragnehmer folgende technische und organisatorische Maßnahmen getroffen worden:

1. Zutrittskontrolle
   Maßnahmen, um Unbefugten den Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

_____

_____

_____

_____

2. Zugangskontrolle
   Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

_____

_____

_____

_____

3. Zugriffskontrolle[5]
   Maßnahmen, um zu gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren 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:

_____

_____

[4] Rechtsgrundlage ist für den Auftraggeber § 6 KDO, für den Auftragnehmer § 9 BDSG

[5] Besonders wichtig ist die Festlegung von Verantwortlichkeiten. Aus unklaren Aufgabenverteilungen, beispielsweise bei der Vergabe von Zugriffsrechten, resultieren Schwachstellen mit hohen Risiken.

_____

_____

4. Weitergabekontrolle

Maßnahmen, um zu gewährleisten dass personenbezogene Daten bei der elektronischen Übertragung oder während des 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:

_____

_____

_____

_____

5. Eingabekontrolle

Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

_____

_____

_____

_____

6. Auftragskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

_____

_____

_____

_____

7. Verfügbarkeitskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

_____

_____

_____

_____

8. Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

_____

_____

_____

_____