Dienstanweisung für Richtlinien zur Löschung und Vernichtung von Informationen

Präambel

Informationen müssen sicher gelöscht oder vernichtet werden, wenn Datenträger und Dokumente ausgesondert oder gesetzliche Aufbewahrungsfristen überschritten werden. Einfaches Zerreißen oder Löschen reicht in der Regel für eine ordnungsgemäße Erfüllung der Löschpflichten nicht aus. Eine geregelte Vorgehensweise hilft dabei, den Missbrauch von gespeicherten Daten zu verhindern. Diese Richtlinie dient dazu, die Beschäftigten für das Thema Löschen oder Vernichten von Daten zu sensibilisieren und zu motivieren. Sie soll Hilfe und Unterstützung bei der Auswahl der richtigen Verfahren und Werkzeuge zur Löschung oder Vernichtung von personenbezogenen und dem Berufsgeheimnis unterliegenden (sog. „schutzbedürftigen“) Daten geben. Welches die geeignete Vorgehensweise zur Löschung oder Vernichtung ist, hängt vom verwendeten Datenträger, dessen Speichertechnologie sowie der Schutzbedürftigkeit der Informationen ab. Gemäß § 27 EKD-Datenschutzgesetz (EKD-DSG) sind Maßnahmen erforderlich, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen.
(Zur besseren Lesbarkeit wird in der Richtlinie nur die männliche Form der Beschäftigen genutzt)

§ 1
Geltungsbereich

(1) Diese Richtlinie gilt für alle Beschäftigten der Evangelischen Kirche in Karlsruhe in allen Pfarrämtern, Werken und Diensten sowie den Kindergärten mit Ausnahme des Diakonischen Werkes. Sie umfasst insbesondere Arbeitnehmer, arbeitnehmerähnliche Personen, Auszubildende, Aushilfen, Hospitanten, Praktikanten und ehrenamtliche Mitarbeiter.

(2) Diese Richtlinie berücksichtigt alle zurzeit gebräuchlichen und in der Evangelischen Kirche in Karlsruhe eingesetzten Datenträger. Hierfür ist zwischen analogen Medien (bspw. Papierakten, Videobänder, Magnetbänder) und digitalen Medien zu unterschieden. Die digitalen Speichermedien teilen sich in elektromagnetische (Festplatten, Disketten), optische (CD-ROM, DVD), und Flash-Speicher (USB-Sticks) auf.

§2

Grundsatz

(1) Gemäß § 21 EKD-DSG sind Daten zu löschen,

a) wenn ihre Speicherung unzulässig ist,

b) ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

(2) An die Stelle der Löschung tritt eine Sperrung, soweit

a) im Fall des § 22 EKD-DSG einer Löschung Rechtsvorschriften, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,

b) Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

c) eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(3) Datenträger ist jedes Medium, auf dem Daten festgehalten werden.

(4) Sowohl analoge als auch digitale Speichermedien sind - unabhängig davon, ob es sich um aktuelle oder archivierte Medien handelt - sicher in einem gesonderten verschlossenen Bereich (bspw. abschließbarer Schrank, Archiv, Safe) aufzubewahren und vor dem Zugriff unbefugter Personen zu schützen.

(5) Wie das Verfahren zur Aktenvernichtung bzw. Datenlöschung genau auszusehen hat, hängt vom Schutzbedarf der betroffenen personenbezogenen bzw. dem Berufsgeheimnis unterliegenden Daten ab. Für die Klassifizierung der Schutzbedürftigkeit wird eine Unterteilung der Daten in die Schutzklassen entsprechend der DIN 66399 empfohlen. Ausgehend von der Möglichkeit, dass Vertraulichkeit, Integrität oder Verfügbarkeit von Geschäftsprozessen oder einer Anwendung verloren gehen können, werden maximale Schäden und Folgeschäden betrachtet, die aus einer solchen Situation entstehen können. Es wird unterschieden zwischen „normalem“, „hohen“ und „sehr hohem“ Schutzbedarf. Eine Beschreibung der einzelnen Schutzbedarfskategorien ist in der Übersicht als **Anlage** dieser Richtlinie zu entnehmen.

(6) Für jede Art von Datenträger ist das gemäß § 3 dieser Richtlinie passende Löschverfahren auszuwählen und verbindlich festzulegen.

(7) Nicht alle Daten sollten mit höchstem Schutzniveau gekennzeichnet werden, da ein höherer Zeitaufwand und höhere Kosten verursacht werden. Es gilt der Grundsatz der Verhältnismäßigkeit.

§ 3

Methoden zur Löschung/Vernichtung

(1) Bei der Entsorgung von Altakten hat der Beschäftigte der Evangelischen Kirche in Karlsruhe zu gewährleisten, dass keine Vermischung der Altakten mit normalem Altpapier erfolgt.

(2) Um eine datenschutzkonforme Vernichtung der Unterlagen sicherzustellen, kann ein geeigneter Schredder nach DIN-Norm 66399 eingesetzt werden. Es sind die in § 2 Abs. 5 dieser Richtlinie genannten Schutzbedarfskategorien zu beachten. Bei größeren Mengen kann ein Entsorgungsunternehmen beauftragt werden, welches sorgfältig auszuwählen ist. Es gelten die Regelungen des § 5 dieser Richtlinie.

(3) Bei Löschung elektronischer Datenbestände sind besondere technische Maßnahmen für die Löschung zu treffen. Informationen auf Datenträgern müssen vor einer Weitergabe (bspw. an einen Reparatur-Dienstleister) oder Aussonderung so gelöscht werden, dass eine Rekonstruktion der Informationen mit hoher Wahrscheinlichkeit ausgeschlossen werden kann. Es ist zu beachten, dass die auf den digitalen Speichermedien gespeicherten Daten grundsätzlich durch die alleinige Nutzung der durch das Betriebssystem bereitgestellten Löschfunktion wieder herstellbar sind. Zur sicheren Löschung sind diese durch physikalische Maßnahmen (mechanische oder thermische Zerstörung, magnetische Durchflutung des Datenträgers) oder mehrmaliges Überschreiben unkenntlich zu machen.

(4) Optische Datenträger (bspw. CD-ROM, DVD) sind einer datenschutzkonformen physikalischen Vernichtung zuzuführen, da eine Überschreibung des Datenbestandes nicht möglich ist.

§ 4

Regelungen zu den Aufbewahrungsfristen

(1) Als Aufbewahrungspflichten kommen Regelungen aus der EKD-Richtlinie über die Aufbewahrung, Aussonderung und Vernichtung (Kassation) von Unterlagen kirchlicher Körperschaften, Einrichtungen, Werke und Stiftungen (Aufbewahrungs- und Kassationsrichtlinie), insbesondere § 2 in Betracht. Darüber hinaus kann die Evangelische Kirche Dokumente bis zum Ablauf der gesetzlichen Verjährung aufbewahren, wenn die Dokumente benötigt werden, um eventuelle Ansprüche abzuwehren.

(2) Weiterhin gelten die jeweiligen berufs- und kirchenrechtlichen Regelungen der Evangelischen Kirche.

(3) Für Ansprüche gegen kirchliche Stellen, die nach Kirchengesetz oder nach anderen kirchlichen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Verarbeitung personenbezogener Daten einen Schaden an der betroffenen Person zu verschulden haben, beträgt die Verjährungsfrist gemäß § 48 Abs. 5 EKD-DSG jene aus § 254 BGB entsprechend.

(4) Personalunterlagen sind ebenfalls unter Berücksichtigung der gesetzlichen Aufbewahrungspflichten zu löschen.

§ 5

Löschung/Vernichtung durch Dritte

(1) Wird die Vernichtung bzw. Löschung von Daten im Rahmen durch einen Dienstleister erledigt, liegt eine Auftragsdatenverarbeitung i.S.d. § 30 EKD-DSG vor.

(2) Auch wenn der Dienstleister den Auftrag zur Vernichtung bzw. Löschung der Daten übernimmt, verbleibt die Verantwortung für den Schutz der betroffenen personenbezogenen Daten weiterhin im Verantwortungsbereich der Evangelischen Kirche in Karlsruhe. Es wird daher empfohlen, mit dem Dienstleister einen Vertrag zur Auftragsdatenverarbeitung abzuschließen und die Einhaltung der technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen.

§ 6

Aktualisierung

(1) Auf Grund der sich ändernden Technologien muss die Richtlinie regelmäßig überarbeitet werden, damit die beschriebenen Lösch- und Vernichtungsmethoden auch für neue Arten von Datenträgern geeignet sind. Gegebenenfalls sind neue Verfahren zu entwickeln und anzuwenden.

(2) Müssen andere, in der Richtlinie nicht erfasste, Datenträger gelöscht werden, ist die Richtlinie soweit möglich sinngemäß anzuwenden.

Karlsruhe, den 12. Juli 2018

Dr. Thomas Schalla
Dekan

Lothar Stängle
Verwaltungsdirektor EKV

Anlage zur Richtlinie Löschung und Vernichtung von Informationen

Schadensbedarfskategorien nach DIN 66399

Schutzbedarf Die Schadens-auswirkungen...	**Schutzklasse 1:** ***Normal* für interne Daten** …sind **begrenzt** und **überschaubar**.	**Schutzklasse 2:** ***Hoch* für vertrauliche Daten** …können **beträchtlich** sein.	**Schutzklasse 3:** ***Sehr Hoch* für besonders vertrauliche und geheime Daten** …können ein existentiell **bedrohliches**, **katastrophales** Ausmaß erreichen.
Verstoß gegen Gesetze/Vorschriften Verstoß gegen Verträge	Verstöße haben **geringe** Konsequenzen. Kleine Vertragsverletzungen nur mit **geringen** Konventionalstrafen	Bei Verstößen drohen **erhebliche** Konsequenzen. Vertragsverletzungen mit **hohen** Konventionalstrafen.	**Fundamentaler** Verstoß gegen Vorschriften und Gesetze. Vertragsverletzungen, deren Haftungsschäden **ruinös** sind.
Beeinträchtigung des informationellen Selbstbestimmungsrechts durch die Verarbeitung	Personenbezogen Daten, bei deren Verarbeitung… …der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen **beeinträchtigt werden kann**.	…der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen **erheblich beeinträchtigt werden kann**.	…eine **Gefahr für Leib und Leben** oder die **persönliche Freiheit des Betroffenen** gegeben ist.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung **erscheint nicht möglich**.	Eine Beeinträchtigung kann **nicht absolut ausgeschlossen** werden.	**Gravierende Beeinträchtigungen** sind möglich. **Gefahr für Leib und Leben**
Beeinträchtigung der Aufgabenerfüllung Max. tolerierbare Ausfallzeit	Die Beeinträchtigung würde von den Betroffenen als **tolerabel** eingeschätzt werden. Diese **ist größer als** 24 Stunden.	Die Beeinträchtigung würde von **einzelnen Betroffenen als nicht tolerabel** eingeschätzt. Diese liegt **zwischen** einer u. 24 Stunden.	Die Beeinträchtigung würde von **allen Betroffenen als nicht tolerabel** eingeschätzt werden. Diese **ist kleiner als** eine Stunde.
Negative Innen- oder Außenwirkung	Eine Ansehens- der Vertrauensbeeinträchtigung ist… …im **geringen** bzw. **nur internen** Umfang zu erwarten.	…im **breiten** Umfang zu erwarten.	…denkbar, evt. sogar in **existenzgefährdender Art**.
Finanzielle Auswirkungen	Der finanzielle Schaden bleibt für die Institution **tolerabel**.	Der Schaden bewirkt **beachtliche,** jedoch **nicht existenzbedrohende**, Verluste.	Der finanzielle Schaden ist für die Institution **existenzbedrohend.**

EVANGELISCHE KIRCHE
IN KARLSRUHE

datenschutz :Leistungen
Mensch. Unternehmen. Werte.

Datenträgervernichtung

1. Definieren Sie Ihre Schutzklasse …

2. … daraus ergeben sich die Sicherheitsstufen.

Schutzklasse 1
Normaler Schutz für interne Daten.

Schutzklasse 2
Hoher Schutzbedarf für vertrauliche Daten.

Schutzklasse 3
Sehr hoher Schutzbedarf für besonders vertrauliche und geheime Daten.

Sicherheitsstufen	Informationen in Originalgröße	Optische Datenträger	Magnetische Datenträger	Elektronische Datenträger	Informationen in verkleinerter Form	Festplatten mit magnetischem Datenträger
Sicherheitsstufe 1: für Datenträger mit allgemeinen Daten, die unlesbar gemacht werden sollen, z. B. Kataloge oder Prospekte o. ä.	P-1	O-1	T-1	E-1	F-1	H-1
Sicherheitsstufe 2: für Datenträger mit internen Daten, die unlesbar gemacht werden sollen, z. B. allgemeine interne Arbeitsanweisungen, Reiserichtlinien, Formulare o. ä.	P-2	O-2	T-2	E-2	F-2	H-2
Sicherheitsstufe 3: für Datenträger mit sensiblen und vertraulichen Daten, z. B. Angebote, Bestellungen mit Adressdaten von Personen	P-3	O-3	T-3	E-3	F-3	H-3
Sicherheitsstufe 4: für Datenträger mit besonders sensiblen und vertraulichen Daten, z. B. Personaldaten, Arbeitsverträge, Bilanzen, Steuerunterlagen von Personen o. ä.	P-4	O-4	T-4	E-4	F-4	H-4
Sicherheitsstufe 5: für Datenträger mit geheim zu haltenden Daten, z. B. medizinische Berichte, Konstruktionspläne, Strategiepapiere o. ä.	P-5	O-5	T-5	E-5	F-5	H-5
Sicherheitsstufe 6: für Datenträger mit geheim zu haltenden Daten, wenn außergewöhnlich hohe Sicherheitsvorkehrungen einzuhalten sind, z. B. Forschungs- und Entwicklungsunterlagen o. ä.	P-6	O-6	T-6	E-6	F-6	H-6
Sicherheitsstufe 7: für Datenträger mit streng geheim zu haltenden Daten, wenn höchste Sicherheitsvorkehrungen einzuhalten sind, z. B. Daten aus geheimdienstlichen oder militärischen Bereichen	P-7	O-7	T-7	E-7	F-7	H-7

DIN-SICHERHEITSSTUFEN

Die Speichermedien, die unsere vertraulichen Daten und Informationen beinhalten, sind vielfältig. Neben dem klassischen Datenträger Papier spielen digitale Datenträger eine wichtige Rolle.
Die DIN-Norm 66399 berücksichtigt diese Vielfalt und definiert die Sicherheit für alle unsere zeitgemäßen Medien. Die DIN 66399 beschreibt die Anforderungen an Maschinen und Prozesse zur Vernichtung von Datenträgern.

Die sechs Unterkategorien:

- **P** Papierprodukte
- **F** Informationen in verkleinerter Form wie Filme, Mikrofiche usw.
- **O** Optische Datenträger wie CD's, DVD's and Blu-ray usw.
- **T** Magnetische Datenträger wie Disketten, Ausweise, magnetische Bänder und Kassetten usw.
- **H** Festplatten mit magentischen Datenträgern, Laptops und externe Festplatten
- **E** Elektronische Datenträger wie Memorysticks, Laufwerke und Mobiltelefone

Die sieben einzelnen Sicherheitsstufen:

- **P = Papierprodukte**
- **P-1 - 12mm Streifen oder max. Partikelgröße von 2.000 mm²**
- **P-2 - 6mm Streifen oder max. Partikelgröße von 800 mm²**
- **P-3 - 2mm Streifen oder max. Partikelgröße von 320 mm²**
- **P-4 - Partikelschnitt von max. 160mm² mit einer Streifenbreite von max. 6mm =6x25mm**
- **P-5 - Partikelschnitt von max. 30mm² mit einer Streifenbreite von max. 2mm =2x15mm**
- **P-6 - Partikelschnitt von max. 10mm² mit einer Streifenbreite von max. 1mm =1x10mm**
- **P-7 - Partikelschnitt von max. max. 5mm² mit einer Streifenbreite von max. 1mm =1x5mm**

Maximale Partikelgröße für andere Datenträger

Klasse	Film	Max mm²	Optisch	Max mm²	Magnetisch	Max mm²	Festplatten	Max mm²	Elektronisch	Max mm²
Kl. 1	**F-1**	**160**	**O-1**	**2000**	**T-1**	**Funktionsuntüchtig**	**H-1**	**Funktionsuntüchtig**	**E-1**	**Funktionsuntüchtig**
	F-2	**30**	**O-2**	**800**	**T-2**	**2000**	**H-2**	**beschädigt**	**E-2**	**zerteilt**
	F-3	**10**	**O-3**	**160**	**T-3**	**320**	**H-3**	**verformt**	**E-3**	**160**
Kl. 2	**F-4**	**2.5**	**O-4**	**30**	**T-4**	**160**	**H-4**	**2000**	**E-4**	**30**
	F-5	**1**	**O-5**	**10**	**T-5**	**30**	**H-5**	**320**	**E-5**	**10**
Kl. 3	**F-6**	**0,5**	**O-6**	**0,5**	**T-6**	**10**	**H-6**	**10**	**E-6**	**1**
	F-7	**0,2**	**O-7**	**0,2**	**T-7**	**2,5**	**H-7**	**5**	**E-7**	**0.5**