Anhang A: Schutzmaßnahmen-Referenzkatalog

V 0.4a (DSK)
Datum: 13.10.2015

Fehlerbereinigte Version nach Vorlage bei der 90. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Gliederung

1. Einleitung

Der Schutzmaßnahmen-Referenzkatalog stellt eine Sammlung von Schutzmaßnahmen dar, die zur Umsetzung der Datenschutz-Gewährleistungsziele herangezogen werden können. Schutzmaßnahmen, die inhaltlich zusammenhängen, werden in Form von Bausteinen gebündelt. Mit Hilfe der Bausteine lassen sich datenschutzrechtliche Anforderungen umsetzen. Da teilweise einzelne Maßnahmen zur Umsetzung mehrerer datenschutzrechtlicher Anforderungen beitragen, gestattet die Gruppierung von Maßnahmen in Bausteinen eine wiederholungsfreie Darstellung, da mehrere Bausteine auf die gleiche Maßnahme verweisen können.

Der Referenzkatalog ist derzeit **im Aufbau begriffen**. Nachfolgend findet sich eine Übersicht über geplante **Maßnahmen-Bausteine** und deren Bearbeitungsstand. Veränderungen an diesem Referenzkatalog erfolgen nach den Vorgaben des Betriebskonzepts des SDM-Handbuches (Stichwort „CR“).

Der **Bearbeitungsstand** ergibt sich wie folgt:

- In Planung ist ein Baustein, welcher von der UAG SDM als „zu erarbeiten“ definiert wurde.
- Im Entwurf ist ein Baustein, für welchen ein Arbeitsstand vorliegt, welcher jedoch unvollständig ist oder vom Bearbeiter für eine weitere Diskussion innerhalb der UAG SDM angemeldet wurde.

- Zur Vorlage ist ein Baustein, welcher von der UAD SDM für eine weitere Bearbeitung/Kommentierung innerhalb des AK Technik und ggf. weiterer AKs freigegeben wurde.
- Freigegeben ist ein Baustein, welcher vom AK Technik und ggf. der Konferenz für eine Verwendung im Schutzmaßnahmen-Referenzkatalog empfohlen wurde.

Der Aufbau der Bausteine folgt einer festgelegten Struktur: Neben einer allgemeinen **Beschreibung**, was mit den Maßnahmen erreicht werden soll, wird nach **Einzelmaßnahmen für die Schutzkomponenten Daten, Systeme und Prozesse differenziert**. Ein weiterer Abschnitt befasst sich mit den Anforderungen, falls sich aus einer Schutzbedarfsanalyse ein **erhöhter Schutzbedarf** ergibt. **Praxisbeispiele** für den öffentlichen und nicht-öffentlichen Bereich sowie **Referenzdokumente** (Orientierungshilfen, Dokumente des BSI, nationale und internationale Standards) werden zur Vertiefung benannt. Zusammenfassend werden die im jeweiligen Baustein adressierten **Einzelmaßnahmen** zusammengestellt, um eine einfache Zuordnung dieser konkreten Einzelmaßnahmen zu den jeweiligen Gewährleistungszielen zu ermöglichen.

Nr.	Überblick der Datenschutz-Bausteine	Status
B.01	Datenvermeidung	In Planung
B.02	Informationsreduktion	In Planung
B.03	DS-gerechtes Datenmodell	In Planung
B.21	Aufbewahrung	Vorlage
B.22	Sperren	Vorlage
B.23	Löschen	Vorlage
B.31	Entgegennahme von Willenserklärungen	Entwurf
B.32	Durchsetzung berechtigter Änderungen	In Planung
B.33	Benachrichtigung der Betroffenen	Entwurf
B.41	Kryptografie	In Planung
B.42	Malwareschutz	In Planung
B.43	Netzwerkschutz	In Planung
B.44	Backup/Recovery	In Planung
B.45	Redundanz sowie Reparatur und Ausweich- oder Ersatzstrategien	In Planung
B.46	Härtung von Systemen	In Planung
B.47	Isolierung	In Planung
B.61	Dokumentation	Entwurf
B.62	Protokollierung	In Planung
B.63	Überwachung	In Planung
B.64	Test & Freigabe	In Planung
B.65	Soll-Ist-Abgleich von Prozessen	In Planung
B.66	Strukturierung von Fachapplikationen	In Planung
B.67	Transaktionssicherung	In Planung
B.81	Datenschutzmanagement	In Planung

Nr.	Überblick der Datenschutz-Bausteine	Status
B.82	IT-Security-Management	In Planung
B.83	Compliance-Management	In Planung
B.84	Rechte- und Rollenkonzept	Entwurf
B.85	Vergleich mit geeigneten Maßnahmen des IT-Grundschutz des BSI	In Planung
B.91	Awareness	In Planung
B.92	Schulung	In Planung

2. Bausteine

Baustein B.21 „Aufbewahrung“

1 Bezug zu Gewährleistungszielen

Verfügbarkeit, Integrität, Intervenierbarkeit, Transparenz

2 Darstellung, Zweck und "Was bedeutet das?"

Die Aufbewahrung von personenbezogenen Daten ist das Bereitstellen dieser Daten zur Verarbeitung und Nutzung für die Dauer der rechtlich gebotenen Speicherpflichten bis zum Zeitpunkt der Aussonderung (Abgabe an Archive oder Vernichtung). Aufbewahrung im hier betrachteten Kontext betrifft Daten, die

- als aktiver Datenbestand nach Ablage zur erneuten Bearbeitung jederzeit einfach wieder verfügbar gemacht werden müssen oder
- als passiver Bestand für das tägliche Geschäft nicht mehr erforderlich sind, aber wegen rechtlich gebotener Speicherpflichten und für Zwecke der Wahrung von Betroffenenrechten noch nicht gelöscht werden dürfen.

Der Zeitraum zwischen Erhebung und erstmaliger Speicherung der Daten und dem Abschluss der Bearbeitung, in dem die Daten für die tägliche Aufgabenerfüllung ständig verfügbar sein müssen (aktiver Bestand), wird hier nicht als Aufbewahrung betrachtet.

Auch nicht betrachtet wird hier die Archivierung von Daten, weil die Abgabe von Daten in Archive gesondert gesetzlich geregelt ist. Archivierung betrifft die Bewertung archivreifer und die Übernahme archivwürdiger Daten, deren Erschließung, dauerhafte Verwahrung und Erhaltung als Archivgut sowie die Bereitstellung der Daten für die Benutzung. Mit der Archivierung geht die datenschutzrechtliche Verantwortung für die Daten von der bisher zuständigen verantwortlichen Stelle an die für das Archiv verantwortliche Stelle über.

Während des Zeitraums der Aufbewahrung von Daten muss sichergestellt sein, dass die Datenobjekte weiterhin genutzt werden können, auch wenn die für das jeweilige Datenformat notwendige Anzeige- oder Bearbeitungs-Software und ggf. die notwendige Hardware nicht mehr Stand der Technik sind und somit in den aktuellen Geschäftsprozessen nicht mehr genutzt werden. Das kann durch folgende Strategien erreicht werden:

a) Die Datenobjekte werden auf Papier ausgedruckt, das dann auf die herkömmliche Weise aufbewahrt wird. Diese Herangehensweise bedeutet jedoch einen Rückschritt aus dem Paradigma der elektronischen Geschäftstätigkeit bzw. Verwaltungsarbeit. Sie ist weder mit den Forderungen der E-Government-Gesetze von Bund und Ländern nach elektronischer Aktenführung noch mit den Bestrebungen der Wirtschaft nach effizienten, elektronischen Geschäftsprozessen vereinbar. Die Variante ist daher nicht zu empfehlen, kann aber für einen zeitlich überschaubaren Übergangszeitraum nicht völlig ausgeschlossen werden.

b) Die bei der erstmaligen Speicherung verwendeten Systeme (Hardware, Betriebssystem, Software-Werkzeuge) werden vorgehalten und für die Dauer der Aufbewahrung gepflegt. Da der Aufwand bei einer steigenden Menge an vorzuhaltenden Systemen zunimmt, ist dieser Ansatz allenfalls als mittelfristige Übergangslösung zu empfehlen.
Hilfreich können dabei Virtualisierungstechniken sein, die es erlauben, veraltete Betriebssysteme und Anwendungssoftware auf moderner Hardware lauffähig zu halten.

c) Die Datenobjekte werden mit Beginn der Aufbewahrung (und ggf. zusätzlich von Zeit zu Zeit während der Aufbewahrung) in neue digitale Repräsentationen überführt (Transformation, Format-Migration). Diese Variante ist auch aus datenschutzrechtlicher Sicht zu empfehlen, da es hier keine Abhängigkeit von einer Vielzahl unterschiedlicher Komponenten gibt und die Datenobjekte in ein Standardformat überführt werden. Sie sind damit unabhängig von der Soft- und Hardwareumgebung, in der sie entstanden sind.

Während des gesamten Zeitraums der Aufbewahrung von personenbezogenen Daten muss gewährleistet sein, dass die Daten lesbar und durch die verantwortliche Stelle weiter verarbeitbar sind, um den datenschutzrechtlichen Anforderungen an Verfügbarkeit, Integrität und Intervenierbarkeit jederzeit genügen zu können. Dies erfordert entsprechende Festlegungen für Daten (Inhalts-, Meta- und Verifikationsdaten), für die technischen Systeme und für die dazugehörigen Prozesse.

Daten

Für den Zeitraum der Aufbewahrung personenbezogener Daten müssen für die Inhaltsdaten die Datenformate, die Syntax und die Semantik detailliert festgelegt und dokumentiert werden. Bei der Wahl der Datenformate ist anzustreben, dass die Daten plattform- und herstellerunabhängig, eindeutig interpretierbar und für die Dauer der gesetzlichen Aufbewahrungsfristen verkehrsfähig sind. Vorteilhaft wäre dabei, wenn die Spezifikationen standardisiert und öffentlich zugänglich sind. Für eine langfristige Ablage der Inhaltsdaten von Dokumenten sind bspw. Formate wie PDF/A, Text (ASCII), ODF, TIFF, JPEG oder PNG geeignet.

Neben den Inhaltsdaten sind Metadaten erforderlich, die helfen, aus Repräsentationen und ihren Daten für den Menschen interpretierbare Informationsobjekte herzustellen. Für den Zeitraum der Aufbewahrung muss festgelegt werden, welche Metadaten in welchen Formaten gemeinsam mit den Inhaltsdaten gespeichert werden. Das betrifft bspw. „beschreibende Metadaten“ wie Aktenzeichen, Betreff, Bezug oder Einsender, „technische Metadaten“ wie Dateiname, Dateiformat, Dateigröße, Hashwerte oder bei Erstellung verwendete bzw. zur Nutzung notwendige Softwareumgebungen oder „administrative Metadaten“ mit Angaben, um die Verwaltung und die Nutzung der Objekte

nachvollziehen zu können. Für eine langfristige Ablage der Metainformationen ist grundsätzlich das XML-Format geeignet.

In bestimmten Fällen ist der Beweiswert von Daten während des Zeitraums der Aufbewahrung zu erhalten. Zu diesem Zweck sind Verifikationsdaten (elektronischen Beweisdaten) erforderlich, die gemeinsam mit den Inhaltsdaten für den Zeitraum der Aufbewahrung gespeichert werden müssen. Diese Daten müssen sämtliche Informationen enthalten, die zur Verifikation der Authentizität und Integrität der gespeicherten Daten, deren Signaturen, Zertifikate und der Signaturerneuerungen benötigt werden. Die hierfür maßgeblichen Rahmenbedingungen sind bspw. in der Technischen Richtlinie TR-03125 des BSI beschrieben.

Technische Systeme

Die eingesetzte Technik muss die datenschutzrechtlichen Anforderungen erfüllen. Dies erfordert eine Abbildung der abstrakten datenschutzrechtlichen Erfordernisse auf eine technische Implementierung entsprechender beweisbar sicher und datenschutzkonform ablaufender IT-Systeme. Die technischen Systeme müssen in der Lage sein, Inhalts-, Meta- und Verifikationsdaten für den gesamten Zeitraum der Aufbewahrung zu erhalten. Zu diesem Zweck sind Maßnahmen erforderlich, die zum Erhalt der im Speichersystem auf physikalischen Speichermedien abgelegten digitalen Objekte geeignet sind. Sofern nicht sichergestellt werden kann, dass die Software- und Hardwareumgebung, in der die Datenobjekte entstanden sind, mittel- und langfristig noch verfügbar sind, müssen die Datenobjekte unabhängig von einer bestimmten Software- und Hardware-Umgebung gemacht werden.

Die technischen Systeme müssen eine dauerhafte physikalische Speicherung gewährleisten. Folgende technische Maßnahmen bezüglich der technischen Systeme können dazu beitragen:

- redundante Vorhaltung der Datenbestände
- räumlich verteilte Speicherung der Daten
- parallele Nutzung unterschiedlicher Speichersysteme (Diversität)
- regelmäßiges Ersetzen von Datenträgern (Refreshment)
- regelmäßige Migration auf andere Speichersysteme (Replication)
- Erhalten der Lauffähigkeit veralteter Software (Betriebssysteme, Anwendungssoftware) durch Virtualisierung
- Etablierung von Sicherungs- und Rücksicherungs-Strategien (Recovery)
- Etablierung von Protokollierungs-Mechanismen
- Umsetzung von Maßnahmen, mit denen gesetzlich geforderte Mandantentrennungen bei einer erneuten Nutzung der Daten gewährleistet werden
- Gewährleistung der Echtheit und Unverfälschtheit von Archivdatenobjekten beim Abruf von Nachweisen, indem die Middleware sämtliche hierfür erforderlichen elektronischen Beweisdaten erstellt und zurückgibt
- Maßnahmen zum Erhalt der Beweiskraft der im Aufbewahrungsspeicher verbleibenden Dokumente beim Löschen anderer aufbewahrter Datenobjekte
- Maßnahmen, die gewährleisten, dass bei einem Löschauftrag sämtliche Daten und Metadaten sowie alle Versionen eines Datenobjektes gelöscht werden

Prozesse

Es sind organisatorische Prozesse erforderlich, die regeln, wer nach welchen Vorgaben und nach welchen rechtlichen Kriterien die Aufbewahrungsdauer festlegt. Zudem muss einmalig zu Beginn der Datenverarbeitung und dann anlassbezogen für die Übernahme der Daten in den Aufbewahrungsspeicher eine Inventur der vorhandenen Formate durchgeführt werden. Auf der Basis dieser Inventur sind Kriterien für die Auswahl der technischen Systeme zur Erhaltung der Daten zu definieren und der Zeitpunkt der Konvertierung in das Aufbewahrungsformat bzw. der Migration auf andere Speichersysteme zu definieren. In diesem Zusammenhang sind auch Prozesse zu definieren, die den Umgang mit versionierten Daten steuern.

Ein Dokumentationsprozess muss sicherstellen, dass auch bei langfristiger Aufbewahrung jederzeit nachvollzogen werden kann, welche Hard- und Software erforderlich ist, um die Daten lesen, interpretieren, verarbeiten und nutzen zu können. Jede Formatkonvertierung und jede Migration auf andere Speichersysteme ist zu protokollieren.

Für die im Rahmen der Datensicherung vorgehaltenen Daten müssen technische und organisatorische Prozesse spezifiziert und implementiert werden, mit denen die Wiederherstellung in geforderten Umfängen binnen vorgegebenen Fristen möglich ist. Dies ist Voraussetzung, um sowohl ein nachträgliches Ändern aufbewahrter Daten (Ändern, Löschen, Sperren) – bspw. als Folge der Intervention Betroffener – als auch die Auskunft an Betroffene zu seinen gespeicherten Daten technisch und organisatorisch zu gewährleisten.

Das Löschen von Daten und Dokumenten vor Ablauf des gesetzlich vorgeschriebenen Aufbewahrungszeitraums muss durch organisatorisch berechtigte Nutzer einer technisch berechtigten vorgelagerten IT-Anwendung angestoßen werden.

Auch das Löschen von Daten und Dokumenten nach Ablauf des gesetzlich vorgeschriebenen Aufbewahrungszeitraums (Ende der maximal zulässigen Speicherdauer) kann durch organisatorisch berechtigte Nutzer einer technisch berechtigten vorgelagerten IT-Anwendung angestoßen werden, oder durch einen zentralen Prozess, der diese Funktion für den gesamten aufbewahrten Datenbestand ausführt und entsprechend berechtigt ist.

3 Differenzierung bei hohem Schutzbedarf

Das Gesamtsystem muss geeignete Maßnahmen vorsehen und implementieren, die einerseits eine unzulässige Manipulation oder den unzulässigen Austausch von Komponenten oder Modulen und die unberechtigte Kenntnisnahme der Daten zuverlässig verhindern und andrerseits die Integrität und Authentizität der Daten gewährleisten. Diese Maßnahmen sind abhängig vom Schutzbedarf der aufbewahrten Daten.

Hoher Schutzbedarf ist in der Regel für die Fälle zu realisieren, bei denen der Beweiswert von Daten während des Zeitraums der Aufbewahrung erhalten werden muss (bspw. bei der elektronischen Speicherung von Urkunden oder Verwaltungsakten). Durch physische Sicherungsmaßnahmen muss die IT-Infrastruktur zur beweiswerterhaltenden Archivierung und die entsprechenden Speichermedien vor Verlust, Zerstörung sowie unberechtigter Veränderung geschützt werden.

4 Beispiele

Abgangs- und Abschlusszeugnisse sowie Prüfungslisten der beruflichen Schulen sind bspw. nach der Schuldatenschutzverordnung Mecklenburg-Vorpommerns 45 Jahre lang aufzubewahren, auch wenn

sie in Form von Dateien gespeichert sind (§ 6 Abs. 1 SchulDSVO M-V). Während des gesamten Zeitraums der Aufbewahrung muss die Schule in der Lage sein, auf Wunsch des Betroffenen Zeugniskopien anzufertigen und herauszugeben.

Daten medizinischer Behandlungen (behandlungsbezogene Dokumente) sind gemäß der Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren (§ 10 Abs. 3 MBO-Ä 1997). Die Deutsche Krankenhausgesellschaft empfiehlt sogar eine 30-jährige Aufbewahrung. Dies ergibt sich aus Gründen der Beweissicherung, da Schadensersatzansprüche, die auf der Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit beruhen gemäß § 199 Abs. 2 Bürgerliches Gesetzbuch (BGB) spätestens in 30 Jahren verjähren, mithin ein Haftungsprozess erst Jahrzehnte nach Beendigung der Behandlung gegen den Krankenhausträger anhängig gemacht werden kann.

5 Referenzen (auf Dokumente, bevorzugt OH, TR)

Orientierungshilfe Dokumentenmanagementsysteme
https://www.datenschutz-mv.de/datenschutz/publikationen/informat/dms/oh_dms.html

Orientierungshilfe Mandantenfähigkeit
https://www.datenschutz-mv.de/datenschutz/publikationen/informat/mandant/oh_mandant.pdf

IT-Planungsrat: Nationale Langzeitspeicherung (NaLa)
http://www.it-planungsrat.de/DE/Projekte/AbgeschlosseneProjekte/NaLa/NaLa_node.html

BSI: TR-03125 (TR-ESOR - Beweiswerterhaltung kryptographisch signierter Dokumente)

DIN: DIN 31644 (Kriterien für vertrauenswürdige digitale Langzeitarchive)
DIN 31645 (Leitfaden zur Informationsübernahme in digitale Langzeitarchive)

ISO: ISO 14721:2012 OAIS Version 2 vom August 2012" (Referenz-Modell für Komponenten, Abhängigkeiten, Funktionen und Prozesse für Lösungen zur Langzeitspeicherung)

6 Zusammenfassung der Maßnahmen

Ebene Daten

B.21 M01 Festlegung geeigneter Datenformate für die aufzubewahrenden Daten
B.21 M02 Festlegung von Art und Umfang der mit aufzubewahrenden Metadaten
B.21 M03 Festlegung von Regeln zum Umgang mit versionierten Daten
B.21 M04 Festlegung aller Verifikationsdaten, die zum Erhalt des Beweiswertes von Daten mit aufbewahrt werden müssen
B.21 M05 Inventur aller vorhandenen Daten-Formate vor der Aufbewahrung

Ebene Technische Systeme

B.21 M31 Ausdruck von aufzubewahrenden Daten auf Papier
B.21 M32 Aufbewahrung von Hard- und Softwarekomponenten für den Zeitraum der Aufbewahrung der damit ursprünglich verarbeiteten Daten
B.21 M33 Transformation aufzubewahrender Daten in neue digitale Repräsentationen
B.21 M34 Redundante Vorhaltung von Datenbeständen

B.21 M35 Räumlich verteilte Speicherung von Daten
B.21 M36 Parallele Nutzung unterschiedlicher Speichersysteme
B.21 M37 Regelmäßiges Ersetzen von Datenträgern (Refreshment)
B.21 M38 Regelmäßige Migration auf andere Speichersysteme
B.21 M39 Einsatz von Virtualierungstechniken zum Erhalt der Lauffähigkeit veralteter Software
B.21 M40 Bereitstellung der erforderlichen elektronischen Beweisdaten durch die Middleware
B.21 M41 Bereitstellung der erforderlichen Protokollierungssysteme

Ebene Prozesse

B.21 M61 Rechtzeitige Festlegung des Zeitpunktes der Konvertierung in das Aufbewahrungsformat bzw. der Migration auf andere Speichersysteme
B.21 M62 Definition der Kriterien für die Auswahl der technischen Systeme zur Erhaltung der Daten
B.21 M63 Erarbeitung von Sicherungs- und Rücksicherungs-Strategien
B.21 M64 Protokollierung jeder Formatkonvertierung
B.21 M65 Protokollierung jeder Migration auf andere Speichersysteme
B.21 M66 Erhalt der Mandantentrennungen aufbewahrter Daten
B.21 M67 Prüfung der Einhaltung vorgegebener Fristen zur Wiederherstellung von Daten
B.21 M68 Erarbeitung eines Rollen- und Rechtekonzeptes für alle Prozesse der Aufbewahrung und Wiederherstellung von Daten

Baustein B.22 „Sperren“

1 Bezug zu Gewährleistungszielen

Intervenierbarkeit, Nichtverkettbarkeit, Integrität, Vertraulichkeit

2 Darstellung, Zweck und "Was bedeutet das?"

Sperren ist das Kennzeichnen von gespeicherten personenbezogenen Daten, um deren weitere Verarbeitung oder Nutzung einzuschränken. Daten sind zu sperren, wenn die gesetzlich geforderte Löschung nicht möglich ist, weil

- der Löschung andere Rechtsvorschriften entgegenstehen,
- die Berichtigung oder Löschung von Daten die Interessen des Betroffenen beeinträchtigen würde,
- eine Löschung wegen der besonderen Art der Speicherung nicht möglich ist oder

wenn der Betroffene es verlangt, weil die Richtigkeit der betreffenden Daten von ihm bestritten wird.

Sperren ist somit einerseits ein wichtiges Werkzeug für verantwortliche Stellen, um Betroffenen die Durchsetzung ihres Rechts auf Intervenierbarkeit zu ermöglichen. Das Sperren dient andererseits der Gewährleistung der Integrität von Datenbeständen, weil unrichtige Daten dem Verarbeitungsprozess entzogen werden können. Da die Verarbeitung oder Nutzung gesperrter Daten eingeschränkt wird, dient diese Maßnahme auch der Gewährleistung der Vertraulichkeit. Schließlich ist Sperren ein Mittel, um die Nichtverkettbarkeit zu unterstützen, weil Daten, die nicht weiter verarbeitet oder

genutzt werden dürfen oder sogar gelöscht werden müssten, nicht mehr für mögliche Verkettungen zur Verfügung stehen.

Wesentliches Ziel der Sperrung ist es, dass nach einer entsprechenden Entscheidung der verantwortlichen Stelle weder Sachbearbeiter noch automatisierte Verfahren die von der Sperrung betroffenen personenbezogenen Daten im regulären Betrieb weiter verarbeiten und nutzen können, obwohl sie in der datenverarbeitenden Stelle physikalisch (in Papierform oder elektronisch gespeichert) noch vorhanden sind. Unter bestimmten Voraussetzungen (z. B. bei Patientendaten, für wissenschaftliche Zwecke, zur Behebung einer Beweisnot) ist eine Verarbeitung gesperrter Daten dennoch möglich.

Es gibt die Möglichkeit, gesperrte Daten unter Beachtung gesonderter Verarbeitungsregeln weiter zu verarbeiten. Gesperrte Patientendaten bspw. dürfen für eine erneute Behandlung verarbeitet werden, wenn sie im Zusammenhang mit einer früheren Behandlung stehen oder nach einer Einwilligung dazu herangezogen werden. Bei solchen Zugriffen sollten Daten nicht entsperrt werden (weil dann wieder sämtliche Nutzungen der entsperrten Daten möglich wären), sondern der zulässige Zugriff auf die gesperrten Daten im Ausnahmefall hat mit separaten technischen Systemen oder Berechtigungen zu erfolgen (siehe dazu unten). Ist ein solcher separater Zugriff nicht möglich und ist der Zugriff nur durch Entsperren zu erlangen, so ist nach der Verarbeitung wieder eine Sperrung anzubringen.

Die Pflicht zur Sperrung entfällt, wenn z. B. die vom Betroffenen behauptete Unrichtigkeit nicht besteht. Unrichtige Daten hingegen sind zu berichtigen bzw. zu löschen oder müssen weiterhin gesperrt bleiben.

In bestimmten Fällen der geschäftsmäßigen Speicherung zum Zwecke der Übermittlung entfällt das Sperren unrichtiger Daten (§ 35 Abs. 6 BDSG). Auf Verlangen des Betroffenen muss ihm in diesen Fällen jedoch die Möglichkeit eingeräumt werden, eine Gegendarstellung beizufügen.

Das Sperren von Daten darf nicht zu negativen Rückschlüssen auf den Betroffenen führen (z. B. Sperrkennzeichen in der Rubrik „Vorstrafen“ für alle lesbar).

Um Sperren realisieren zu können, sind Maßnahmen auf der Ebene der Daten, der technischen Systeme und der dazugehörigen Prozesse erforderlich.

<u>Daten</u>

Die Struktur der Daten und die Art der Speicherung müssen so gestaltet sein, dass entweder Sperrkennzeichen an einzelnen Datenfeldern angebracht werden können oder dass eine Methode anwendbar ist, mit welcher festgestellt werden kann, ob die Daten gesperrt sind (bspw. durch getrennte Speicherung gesperrter und nicht gesperrter Daten). Ist absehbar, dass größere Dateneinheiten gemeinsam gesperrt werden müssen, können sich das Sperrkennzeichen bzw. die Erkennungsmethode ggf. auch auf Datensatzebene oder auf noch größere Datenmengen beziehen.

Die Struktur der Daten und das Datenmodell müssen so organisiert werden, dass gesperrte Daten vor der geplanten Verarbeitung oder Nutzung erkannt und von der Verarbeitung und Nutzung ausgenommen oder ggf. nach anderen Regeln verarbeitet und genutzt werden können als nicht gesperrte. Bspw. können gesperrte Daten von nicht gesperrten getrennt und in einem separaten Datenbestand gespeichert werden. Möglich ist auch das Anfertigen einer Kopie des gesamten

Datenbestandes, in der gesperrte Daten gelöscht werden und der dann für die weitere Verarbeitung und Nutzung zur Verfügung steht. Auch Verfahren zur teilweisen Trennung der Inhaltsdaten von identifizierenden Daten im Sinne einer Pseudonymisierung sind anwendbar, um die gewünschte Sperrwirkung zu erzielen. Schließlich können Daten auch gesperrt werden, indem sie verschlüsselt werden und der Schlüssel nur besonders berechtigten Personen der Daten verarbeitenden Stelle zugänglich ist.

Sofern unrichtige Daten etwa für Zwecke der Übermittlung gespeichert werden, muss das Datenmodell so organisiert sein, dass Betroffene eine Gegendarstellung hinzuspeichern lassen können, die dann immer gemeinsam mit den Daten zu übermitteln ist (§ 35 Abs. 6 BDSG).

Alle Forderungen in Bezug auf die Sperrung von Daten müssen auch bei allen Kopien und Backups umgesetzt werden können. Das bedeutet jedoch nicht, dass in jeder Kopie und jedem Backup nachträglich Sperrkennzeichen an einzelnen Datenfeldern angebracht werden müssen. Vielmehr sind Methoden einzusetzen, die bei der vorgesehenen Wiederverwendung der Daten nach einem Restore erkennbar machen, welche Daten gesperrt sind und auf diese Weise die Verarbeitung oder Nutzung gesperrter Daten verhindern.

Werden personenbezogene Daten in Akten gesperrt reicht es nicht aus, die einzelnen Dokumente als gesperrt zu kennzeichnen (z. B. mit einem entsprechenden Aufdruck „Gesperrt“). Die gesperrten Dokumente sind der Akte zu entnehmen und entsprechend gekennzeichnet separat abzulegen. Ggf. ist die Entnahme der Dokumente in geeigneter Weise zu protokollieren. Dabei ist sicherzustellen, dass die Sperrkennzeichen nicht zu negativen Rückschlüssen auf den Betroffenen führen dürfen.

Technische Systeme

Die technischen Systeme müssen so ausgestaltet werden, dass sie vor der automatisierten Verarbeitung personenbezogener Daten die Existenz gesperrter Daten erkennen und deren Verarbeitung verhindern. Das betrifft auch Datenbestände aus Sicherungen oder Backups. Dies erfordert ein Zusammenwirken des Sperrkennzeichens bzw. der Methode zur Erkennung von Sperrungen mit weiteren technischen Maßnahmen etwa nach § 9 BDSG. Im Ergebnis müssen die technischen Systeme sicherstellen, dass die vom Gesetz verlangte und von der verantwortlichen Stelle mit der Sperrung angeordnete Verarbeitungs- und Nutzungsbeschränkung auch tatsächlich wirkt.

Um gesperrte Daten nach unterschiedlichen Regeln verarbeiten zu können, ist es hilfreich, wenn die technischen Systeme gesperrte Daten getrennt speichern können. Die Systeme müssen für gesperrte Datenbestände andere Verarbeitungsregeln bereitstellen können als für nicht-gesperrte. Ggf. müssen getrennte technische Systeme für gesperrte und nicht-gesperrte Daten verwendet werden.

Um gesetzlich vorgegebene Sperrfristen automatisiert überwachen zu können (bspw. gem. § 25 Abs. 2 DSG M-V), müssen technische Systeme entsprechende Zeitstempelsysteme beinhalten oder nutzen können. Sind die gesperrten Daten mit entsprechenden Attributen versehen, müssen die technischen Systeme geeignete Auswertemöglichkeiten bereitstellen, mit denen die Fristen überwacht werden.

Sofern Sperrungen nach bestimmten systematischen Vorgaben erfolgen, sollten die technischen Systeme den Vorgang des Sperrens automatisiert durchführen können.

Prozesse

Es ist ein Rechte- und Rollenkonzept erforderlich, auf dessen Basis ein organisatorischer Prozess steuert, welche Personen der verantwortlichen Stelle für die Prüfung und Vergabe von Sperrkennzeichen und für die aus der Sperrung resultierenden weiteren Aufgaben zuständig sind. Da sich das Sperren personenbezogener Daten auch auf einen bestimmten Personenkreis bzw. bestimmte Rollen beziehen kann, müssen Sperrprozesse und deren Auswirkungen auch rollen- und rechteabhängig konfigurierbar sein.

Basis für den ordnungsgemäßen Umgang mit Sperrungen ist ein Sperrkonzept, das in jeder verantwortlichen Stelle vorliegen muss.

Für den technischen Vorgang des Sperrens muss ein Prozess eingerichtet werden, der die logische/physikalische Kennzeichnung bzw. Bearbeitung der zu sperrenden Daten vornimmt (bspw. Setzen eines Sperrkennzeichens oder Attributes, Verschlüsselung der zu sperrenden Daten). Sofern Sperrungen nach fest vorgegeben Regeln erfolgen (etwa Sperrung von Daten bestimmter Zeitscheiben), sollten diese Prozesse nach Möglichkeit automatisiert erfolgen.

Der weitere Umgang mit gesperrten Daten hängt vom Einzelfall ab. Ggf. kann auch der Prozess zur Erzeugung einer Kopie ohne gesperrte Daten, der für die weitere Verarbeitung uneingeschränkt zur Verfügung steht, automatisiert werden. Dabei muss jedoch sichergestellt werden, dass der Bestand mit gesperrten Daten nicht völlig der Verarbeitung entzogen werden darf, da auch gesperrte Daten weiterhin Löschfristen unterliegen, ggf. berichtigt oder sogar weiter verarbeitet werden müssen.

Die standardmäßig vorhandenen Prozesse zur Verarbeitung der Daten müssen so gestaltet sein, dass sie die Tatsache der Sperrung einzelner Daten erkennen und für gesperrte Daten ggf. besondere Verarbeitungsregeln bereitstellen.

Im Zusammenhang mit der Sperrung personenbezogener Daten treffen die verantwortlichen Stellen einige Informationspflichten, die in einem organisatorischen Prozess abgebildet werden müssen. So sind Empfänger von Daten zu informieren, wenn nach der Übermittlung Daten gesperrt wurden (§ 20 Abs. 8 BDSG, § 35 Abs. 7 BDSG, § 13 Abs. 7 DSG M-V).

In bestimmten Konstellationen sind Prozesse erforderlich, die Fristen der Geltung der Sperrung überwachen und sie ggf. automatisiert aufheben (§ 25 Abs. 2 DSG M-V).

Wird Betroffenen das Recht zur Gegendarstellung eingeräumt (etwa falls unrichtige Daten nicht gesperrt werden - § 35 Abs. 6 BDSG) sind Prozesse erforderlich, die vor der Übermittlung dieser Daten das Vorhandensein von Gegendarstellungen prüfen und die Übermittlung ohne Gegendarstellung verhindern.

3 Differenzierung bei hohem Schutzbedarf

Der Schutzbedarf von Daten, die gesperrt werden sollen oder die bereits gesperrt sind, kann erheblichen Einfluss auf die Pflichten der verantwortlichen Stelle in verschiedenen Phasen des Sperrvorgangs haben. Die verantwortliche Stelle hat hier Abwägungsprozesse zu treffen, die sowohl die Sensibilität der Daten als auch die Beeinträchtigung der Rechte der Betroffenen einbeziehen.

Ob die verantwortliche Stelle eine Sperrung anstelle einer Löschung überhaupt anweisen darf, hängt u. a. von der Art der Speicherung der zu löschenden Daten ab. Wenn nur wegen einer „besonderen

Art der Speicherung“ das Löschen mit unverhältnismäßigem Aufwand verbunden wäre, darf anstelle der Löschung gesperrt werden. Für Daten mit hohem Schutzbedarf wäre auch ein hoher Aufwand zur Löschung der Daten angemessen und eine Sperrung käme möglicher Weise nicht in Betracht.

Ob ein Sperrkennzeichen tatsächlich zur wirksamen technischen Umsetzung führt und die weitere Verarbeitung und Nutzung des gesperrten Datums herbeiführt, hängt von der Qualität der gewählten technischen und organisatorischen Maßnahmen ab. Je höher der Schutzbedarf der zu sperrenden Daten ist, umso aufwändiger müssen diese Maßnahmen sein. Die Sperrung von Adressdaten eines Kunden eines Versandunternehmens für Zwecke der Werbung ist durch Setzung eines Kennzeichens möglich und erfordert somit weniger technischen Aufwand als die Sperrung von medizinischen Behandlungsdaten im Krankenhaus nach Abschluss der entsprechenden Behandlung, die bspw. durch getrennte Speicherungen umgesetzt werden kann.

Auch die gesetzlich vorgeschriebene Benachrichtigung von Stellen, an die gesperrte Daten übermittelt wurden, ist vom damit verbundenen Aufwand abhängig. Auch hier gilt, dass die Wahrscheinlichkeit zur Benachrichtigungspflicht steigt, je höher der Schutzbedarf der betroffenen Daten ist.

4 Beispiele

Sperrungen spielen im Zusammenhang mit Patientendaten eine wichtige Rolle. So sind nach dem Landeskrankenhausgesetz M-V Patientendaten in Krankenunterlagen nach Abschluss der Behandlung zu sperren. Die gesperrten Daten sind gesondert zu speichern. Ist die gesonderte Speicherung nicht möglich, sind die Daten mit einem Sperrvermerk zu versehen (§ 37 LKHG M-V).

In einigen Bundesländern ist es erlaubt, dass Lehrer Daten von Schülern auf privater IT-Technik verarbeiten (z. B. § 70 Abs. 4 Schulgesetz M-V). Die dazugehörige Verordnung in Mecklenburg-Vorpommern schreibt bspw. vor, dass diese Daten spätestens ein Jahr, nachdem der Lehrer die Schüler nicht mehr unterrichtet, zu sperren sind.

5 Referenzen (auf Dokumente, bevorzugt OH, TR)

Orientierungshilfe Krankenhausinformationssysteme
https://www.datenschutz-mv.de/datenschutz/publikationen/informat/kis/OH_KIS.pdf

6 Zusammenfassung der Maßnahmen

Ebene Daten

B.22 M01 Schaffung von Datenfeldern für Sperrkennzeichen
- auf Feldebene
- auf Datensatzebene
- auf der Ebene größerer Datenmengen

B.22 M02 Schaffung von Datenfeldern für Sperrfristen
- auf Feldebene
- auf Datensatzebene
- auf der Ebene größerer Datenmengen

B.22 M03 Trennung von Inhalts- und identifizierenden Daten

B.22 M04 Kryptographische Verschlüsselung gesperrter Daten

B.22 M05 Separate elektronische Speicherung von gesperrten und nicht gesperrten Daten

B.22 M06 Entnahme gesperrter Dokumente aus einem Gesamtdatenbestand und separate Ablage
B.22 M07 Inhaltsneutrale Formulierung von Sperrvermerken
B.22 M08 Anfertigen von Datenkopien ohne gesperrte Daten zur weiteren Verarbeitung

Ebene Technische Systeme

B.22 M31 Nutzung getrennter technischer Systeme für die Verarbeitung gesperrter und nicht gesperrter Daten
B.22 M32 Bereitstellung technischer Systeme zur automatisierten Umsetzung von Sperrungen
B.22 M33 Bereitstellung von Zeitstempelsystemen oder vergleichbaren Auswertesystemen zur Überwachung und Steuerung von Sperrfristen
B.22 M34 Bereitstellung von Verschlüsselungssystemen

Ebene Prozesse

B.22 M61 Festlegung von Regeln für die weitere Verarbeitung gesperrter Daten
B.22 M62 Festlegung unterschiedlicher Verarbeitungsregeln für gesperrte und nicht gesperrte Daten
B.22 M63 Festlegung von Regeln für die Rücknahme von Sperrungen
B.22 M64 technische und organisatorische Regelungen für die Anbringung von Gegendarstellungen an fehlerhafte Daten
B.22 M65 Bereitstellung von Prüfmethoden zur Feststellung des Sperrzustandes von Daten
B.22 M66 Erarbeitung eines Rechte- und Rollenkonzeptes für den Umgang mit Sperrungen
B.22 M67 Erarbeitung eines Sperrkonzeptes
B.22 M68 Prozess zur technischen Umsetzung von Sperrungen
B.22 M69 Prozess zur Information der Empfänger von Daten bei nachträglicher Sperrung
B.22 M70 Prozess zur Information Betroffener über die dauerhafte Speicherung falscher Daten und über die Möglichkeit der Gegendarstellung

Baustein B.23 „Löschen“

1 Bezug zu Gewährleistungszielen

Datensparsamkeit, Vertraulichkeit, Intervenierbarkeit, Nichtverkettbarkeit

2 Darstellung, Zweck und "Was bedeutet das?"

Löschen ist das dauerhafte Unkenntlichmachen von gespeicherten personenbezogenen Daten. Daten sind zu löschen, wenn

- sie unrichtig sind und die verantwortliche Stelle keine Kenntnis der unrichtigen Daten erlangen kann,
- ihre Erhebung unzulässig war,
- ihre Speicherung unzulässig ist oder
- ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

Verantwortliche Stellen haben Daten grundsätzlich unaufgefordert (ohne Antrag oder sonstige verfahrenseinleitende Maßnahmen) zu löschen, da sie sich immer an Regelfristen für die Löschung von Daten zu halten haben (vgl. § 4e Satz 1 Nr. 7 BDSG), die sich aus den gesetzlich vorgegebenen, maximalen Speicherfristen ergeben. Mit der Verpflichtung zur Löschung korrespondiert aber auch ein Anspruch des Betroffenen zur Löschung seiner Daten.

Die Pflicht zur Löschung betrifft nicht nur den aktiven Datenbestand sondern auch Daten in Sicherungskopien. Der Löschpflicht unterliegen zudem Protokolldaten, die besonderen Zweckbindungen unterliegen und für die in der Regel gesonderte Speicherfristen gelten. Schließlich ist auch darauf zu achten, dass aus verarbeitungstechnischen Gründen erzeugte temporäre Dateien fristgerecht gelöscht werden. Die verantwortliche Stelle muss zudem sicherstellen, dass die Löschpflichten für die Datenbestände eingehalten werden, die bei ihren Auftragnehmern verarbeitet werden. Dies erfordert vertragliche Regelungen und verbindliche Weisungen.

Der Vorgang des Löschens muss auf irreversible Weise bewirken, dass aus den gelöschten Daten keine Informationen mehr gewonnen werden können. Damit dient das Löschen der Umsetzung mehrerer Gewährleistungsziele. Dass das Löschen von Daten das Gewährleistungsziel Datensparsamkeit unterstützt ist selbstverständlich. Gelöschte Daten stehen zudem auch nicht mehr für mögliche Verkettungen zur Verfügung (Nichtverkettbarkeit). Das Löschen dient auch der Gewährleistung der Intervenierbarkeit, weil Betroffenen die Möglichkeit gegeben wird, falsche oder unzulässig bzw. zu lange gespeicherte Daten löschen zu lassen. Das Löschen von Daten ist aber auch eine technisch-organisatorische Maßnahme zur Gewährleistung der Datensicherheit, insbesondere zur Verhinderung der Kenntnisnahme personenbezogener Daten durch Unbefugte und dient somit auch der Sicherung der Vertraulichkeit. Insofern sind die entsprechenden Regelungen des Bundesdatenschutzgesetzes (§ 9 BDSG sowie dessen Anlage), der Landesdatenschutzgesetze (z. B. § 21 DSG M-V, § 10 DSG NRW, Art. 7 BayDSG) sowie spezialgesetzliche Vorschriften (z. B. § 78a SGB X) zu beachten. Danach müssen die Maßnahmen dem Schutzbedarf der Daten angemessen sein. Ihre Umsetzung hat sich nach den im Einzelfall zu betrachtenden Risiken und dem Stand der Technik zu richten.

In Abhängigkeit von der Sensibilität der zu löschenden Daten, der Menge der zu löschenden Daten und der Art der Datenträger kommen daher verschiedene Methoden in Betracht:

- Überschreiben, Ausstreichen oder Schwärzen von auf Papier gespeicherter Daten,
- Austragen aus elektronischen Verzeichnissen bzw. Tabellen bspw. durch Löschbefehle von Betriebssystemen (z. B. Delete, Erase)*,
- Formatieren von Datenträgern*,
- Überschreiben der Informationen einzelner Datenfelder (Daten oder Attribute von Daten) mit Hilfe von speziellen Löschprogrammen (so genannte Wipe-Tools) ,
- komplettes Überschreiben ganzer Datenträger mit speziellen Löschprogrammen,
- Entfernen des Personenbezugs durch wirksames Anonymisieren,
- Vernichten des Verschlüsselungsschlüssels von verschlüsselt gespeicherten Daten**,
- physikalische Zerstörung des Datenträgers (bspw. Papier, Festplatten, SSD-Speicher) durch mechanisches Zerkleinern (Schreddern) oder Verbrennen.

*) Diese Maßnahmen genügen den gesetzlichen Löschanforderungen selbst bei normalem Schutzbedarf in der Regel nicht, solange nicht weitere Maßnahmen etwa zum Umgang mit den betreffenden Datenträgern umgesetzt werden (siehe Anmerkungen im Abschnitt 3 - Differenzierung bei hohem Schutzbedarf).

**) Dies ist abhängig vom Kryptokonzept, siehe weitere Anmerkungen im Abschnitt 3 - Differenzierung bei hohem Schutzbedarf

Um eine Löschung von Daten zu bewirken, reichen folgende beispielhaft aufgezählte Maßnahmen nicht aus:

- Freigabe von Datenträgern (z. B. eines USB-Sticks) zur Wiederverwendung durch Organisationsanweisung ,
- Aussprechen eines Verbots der Kenntnisnahme und Nutzung der Daten an Mitarbeiter der verantwortlichen Stelle,
- Zusage der verantwortlichen Stelle, Daten nicht mehr verwenden zu wollen.

Um Daten wirksam löschen zu können, sind Maßnahmen auf der Ebene der Daten, der technischen Systeme und der dazugehörigen Prozesse erforderlich.

Daten

Die Struktur der Daten und die Art der Speicherung müssen so gestaltet sein, dass das Löschen der Inhalte einzelner Datenfelder, Datensätze oder vorher definierter Gruppen von Daten möglich ist.

Die Struktur der Daten und das Datenmodell müssen so organisiert werden, dass einzelne Datenfelder, Datensätze oder Gruppen von Daten gelöscht werden können, ohne die Integrität des verbleibenden Datenbestandes zu beeinträchtigen und ohne besondere Zweckbindungsregelungen (bspw. von Protokolldaten, die der Datenschutzkontrolle dienen) zu beeinträchtigen.

Alle Forderungen in Bezug auf die Löschung von Daten müssen auch bei allen Kopien und Backups umgesetzt werden können. Das bedeutet jedoch nicht, dass in jeder Kopie und jedem Backup nachträglich gelöscht werden muss. Vielmehr sind Methoden einzusetzen, die bei der vorgesehenen Wiederverwendung der Daten nach einem Restore erkennbar machen, welche Daten im Originaldatenbestand gelöscht sind und auf diese Weise die Verarbeitung oder Nutzung der in der Kopie oder im Backup noch nicht gelöschten Daten verhindern.

Technische Systeme

Die technischen Systeme zur Umsetzung der von der verantwortlichen Stelle angeordneten Löschung hängen neben dem Schutzbedarf maßgeblich von der Art und Weise des jeweiligen Datenträgers ab, auf dem die Daten gespeichert sind. Sie müssen in jedem Fall so gestaltet sein, dass sie die gesetzlich geforderten Löschvorgänge technisch realisieren können. Im Ergebnis müssen die technischen Systeme sicherstellen, dass der vom Gesetz verlangte und von der verantwortlichen Stelle mit der Löschung angeordnete Informationsverlust auch tatsächlich wirkt. Die Maßnahme M 2.167 der BSI-Grundschutzkataloge beschreibt geeignete Verfahren zur Löschung oder Vernichtung von Daten auf unterschiedlichen Datenträgern.

Die technischen Systeme müssen in der Lage sein, Löschungen durchzuführen, ohne die Integrität des verbleibenden Datenbestandes zu beeinträchtigen. Dazu gehört auch, dass die unbefugte Löschung verhindert wird.

Um gesetzlich vorgegebene Löschfristen automatisiert überwachen zu können, müssen technische Systeme entsprechende Zeitstempelsysteme beinhalten oder nutzen können. Sind die gelöschten Daten mit entsprechenden Attributen versehen, müssen die technischen Systeme geeignete Auswertemöglichkeiten bereitstellen, mit denen die Löschfristen überwacht werden.

Sofern Löschungen nach bestimmten systematischen Vorgaben erfolgen, sollten die technischen Systeme den Vorgang des Löschens automatisiert durchführen können.

Bei der Auswahl technischer Systeme zur Vernichtung von Datenträgern sollte die DIN 66399:2012 "Vernichten von Datenträgern" berücksichtigt werden.

Prozesse

Die verantwortliche Stelle muss in einem Löschkonzept festlegen, wie sie die datenschutzrechtlichen Pflichten zur Löschung personenbezogener Daten erfüllen will.

Es ist ein Rechte- und Rollenkonzept erforderlich, auf dessen Basis ein in einem Löschkonzept beschriebener organisatorischer Prozess steuert, welche Personen der verantwortlichen Stelle für die Prüfung, Anordnung und Durchführung von Löschungen zuständig ist.

Da sich das Löschen personenbezogener Daten auch auf einen bestimmten Personenkreis bzw. bestimmte Rollen innerhalb und außerhalb der verantwortlichen Stelle beziehen kann, müssen Löschprozesse auch rollen- und rechteabhängig konfigurierbar sein.

Das Löschen durch Vernichten von Datenträgern erfordert Prozesse, die abhängig von der Art der zu vernichtenden Datenträger und vom Schutzbedarf der zu löschenden Daten sind. Daher ist ein organisatorischer Prozess erforderlich, der die Auswahl geeigneter Vernichtungsmechanismen steuert.

Sofern das Löschen nach fest vorgegeben Regeln erfolgt (etwa Löschen von Daten bestimmter Zeitscheiben), sollten diese Prozesse automatisiert ablaufen. In diesem Zusammenhang sind weitere Prozesse erforderlich, die jederzeit ein gezieltes Beenden automatisierter Löschprozesse ermöglichen.

3 Differenzierung bei hohem Schutzbedarf

Grundsätzlich ist das Löschen ein irreversibler Prozess. Der Informationsgehalt gelöschter Daten darf nicht reproduzierbar sein. Die technischen und organisatorischen Maßnahmen zum Löschen müssen jedoch dem Schutzbedarf der Daten angemessen sein. Diese grundsätzliche Forderung berücksichtigt bspw. die DIN 66399 („Vernichten von Datenträgern“), indem sie jeder verantwortlichen Stelle empfiehlt, alle im Geschäftsverkehr vorkommenden oder anfallenden Informationen (Daten) bzw. die sie speichernden Datenträger zunächst hinsichtlich des Schutzbedarfs in drei Schutzklassen zu klassifizieren. Sieben Sicherheitsstufen beschreiben zudem Anforderungen an die Wirksamkeit der Vernichtung, d. h. die Höhe des Aufwands für Angreifer, vernichtete Datenträger bzw. darauf gespeicherte Daten wiederherzustellen und Information zur Kenntnis nehmen zu können. Die DIN empfiehlt, Datenträger bestimmter Schutzklassen nur nach bestimmten Sicherheitsstufen zu vernichten und trägt so dem o. g. Prinzip der Angemessenheit Rechnung.

Die Klassifizierung der zu löschenden Daten nach dem Schutzbedarf der betreffenden Daten ist auch bei der Auswahl von Löschmechanismen für elektronisch gespeicherte Daten erforderlich. Für

elektronisch gespeicherte personenbezogene Daten mit geringem Schutzbedarf wird oft das Löschen mit dem Delete-Befehl oder das Formatieren des Datenträgers als angemessene Maßnahme angesehen. Derartige Maßnahmen können selbst für wenig sensible Daten nur dann den gesetzlichen Löschforderungen genügen, wenn der weitere Umgang mit den betreffenden Datenträgern geregelt ist. Aber schon bei normalem Schutzbedarf reichen diese Maßnahmen in der Regel nicht aus, um diesen gesetzlichen Anforderungen gerecht zu werden. Eine angemessene Maßnahme wäre in diesen Fällen bspw. das gezielte Überschreiben zu löschender Speicherbereiche oder ein Überschreiben des gesamten Datenträgers mit Hilfe spezieller Löschprogramme. Das Löschen des Schlüssels verschlüsselt gespeicherter Daten reicht in der Regel nicht aus, um Daten mit hohem oder sehr hohem Schutzbedarf zu löschen. In diesen Fällen bleibt nur das Vernichten der Datenträger durch Schreddern oder fachgerechtes thermisches Vernichten.

Konkrete Empfehlungen zu verwendbaren Löschprogrammen gibt bspw. das BSI in seinen Veröffentlichung „BSI für Bürger“. Auch die Maßnahme M 2.433 der BSI-Grundschutzkataloge gibt einen Überblick über Methoden zur Löschung und Vernichtung von Daten und differenziert dabei nach dem Schutzbedarf der zu löschenden Daten.

4 Beispiele

Die Unterlagen zu medizinischen Behandlungen (Anamnese, Aufnahme- und Aufklärungsbögen, Befunde, Medikation, Pflegeanordnungen, Arztbriefe, EKG, EEG, CTG, histologische Berichte, OP-Berichte usw.) sind gemäß § 10 Abs. 3 MBO (Stand 2011) bzw. § 630f BGB frühestens 10 Jahre nach Abschluss der Behandlung zu löschen. Dabei handelt es sich um besonders schutzbedürftige Daten, die in die beiden höchsten Klassen 2 oder 3 der Schutzklassendefinition der DIN 66399 einzustufen sind und demnach entsprechend aufwendige Löschmechanismen erfordern.

Arbeitgeber sind gemäß § 16 Abs. 2 ArbZG verpflichtet, die über die werktägliche Arbeitszeit hinausgehende Arbeitszeit der Arbeitnehmer aufzuzeichnen. Die Nachweise sind nach zwei Jahren zu löschen. Hier handelt es sich um weniger schutzbedürftige Daten, die in Klasse 1 der Schutzklassendefinition der DIN 66399 einzustufen sind und deren Löschung mit weniger aufwendigen Verfahren angemessen wäre.

Mit der Einstellung des Verfahrens zur Speicherung elektronischer Einkommensnachweises ELENA war die Rechtsgrundlage für die (verschlüsselte) Speicherung der Einkommensnachweise entfallen und die Löschung erforderlich. Angesichts der Sensibilität und der Menge der im Verfahren gespeicherten Daten wurde es als nicht ausreichend angesehen, lediglich die Verschlüsselungsschlüssel zu vernichten. Als angemessene Maßnahme wurde die physikalische Löschung der verschlüsselten Daten gesehen.

5 Referenzen

Hinweise zur Ermittlung des Schutzbedarfs personenbezogener Daten für den Prozess der Datenträgervernichtung
https://www.datenschutz-mv.de/datenschutz/publikationen/informat/datentraeger/vernichtung.pdf

BSI: https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/RichtigLoeschen/richtigloeschen_node.html

M 2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten
M 2.433 Überblick über Methoden zur Löschung und Vernichtung von Daten
M 2.435 Auswahl geeigneter Aktenvernichter
M 2.436 Vernichtung von Datenträgern durch externe Dienstleister
M 4.32 Physikalisches Löschen der Datenträger vor und nach Verwendung

DIN: DIN 66399 Teil 1 und Teil 2

6 Zusammenfassung der Maßnahmen

Ebene Daten

B.23 M01 Festlegung von Datenstrukturen und Speicherarten, die das Löschen der Inhalte einzelner Datenfelder, Datensätze oder vorher definierter Gruppen von Daten ermöglichen
B.23 M02 Organisation der Strukturen von Daten und Datenmodellen dergestalt, dass das Löschen der Inhalte einzelner Datenfelder, Datensätze oder vorher definierter Gruppen von Daten die Integrität der verbleibenden Daten nicht gefährdet
B.23 M03 Entfernen des Personenbezugs durch Anonymisieren

Ebene Technische Systeme

B.23 M31 Austragen von Daten aus Zuordnungstabellen durch Löschbefehle wie Delete oder Erase (weitere Behandlung der betreffenden Datenträger erforderlich)
B.23 M32 Formatieren des Datenträgers mit zu löschenden Daten (weitere Behandlung der betreffenden Datenträger erforderlich)
B.23 M33 Überschreiben von Daten, Datenfeldern, Datenattributen oder kompletten Datenträgern mit speziellen Löschprogrammen (Wipe-Tools)
B.23 M34 Einsatz von Schreddern zur physikalischen Vernichtung von Datenträgern jeder Art
B.23 M35 Verbrennen von Datenträgern jeder Art
B.23 M36 Automatisierte Überwachung von Löschfristen unter Nutzung von Zeitstempelsystemen oder Auswerteverfahren für entsprechende Löschattribute
B.23 M37 Einsatz automatisierter, zeitgesteuerter Löschroutinen unter Nutzung von Zeitstempelsystemen oder Auswerteverfahren für entsprechende Löschattribute
B.23 M38 Einsatz von technischen Systemen, die bei einem Restore von Datenbeständen aus Backups oder Datensicherungen sicherstellen, dass Daten, die im Original gelöscht wurden, nicht weiter genutzt oder verarbeitet werden

Ebene Prozesse

B.23 M61 Erstellung eines Rechte- und Rollenkonzeptes
B.23 M62 Erstellung eines Löschkonzeptes
B.23 M63 Klassifizieren von Daten hinsichtlich des Schutzbedarfs als Voraussetzung zur Auswahl geeigneter Lösch- und Vernichtungsverfahren

B.23 M64 Regelungen mit besonderen Löschvorgaben für Protokolldaten unter Berücksichtigung der speziellen Aufbewahrungs- und Zweckbindungsvorgaben

B.23 M65 Prozess zur Auswahl geeigneter Lösch- und Vernichtungsverfahren unter Berücksichtigung der Empfehlungen des BSI (BSI-Maßnahmen M 2.167, M 2.433 und „BSI für Bürger“) und der Vorgaben der DIN 66399:2012 (Vernichtung von Datenträgern)

B.23 M66 Regeln zum Umgang mit Datenträgern, auf denen Daten lediglich mit Löschbefehlen wie Delete oder Erase aus Tabellen ausgetragen, also nicht physikalisch gelöscht wurden

B.23 M67 Regeln zum Umgang mit Datenträgern, auf denen Daten lediglich durch Formatierung des Datenträgers gelöscht wurden

B.23 M68 Regelungen zum Löschen von Daten, die im Rahmen der Datenverarbeitung im Auftrag bei Auftragnehmern gespeichert sind

B.23 M69 Regelungen zum Umgang mit Verschlüsselungsschlüsseln von zu löschenden (verschlüsselten) Daten

B.23 M70 Organisatorische Vorgaben zum Überschreiben, Ausstreichen oder Schwärzen von auf Papier gespeicherten Daten