Baustein 11 „Aufbewahrung“

Version: V1.0
Bezugsquelle: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Hinweis: Dieser Baustein wurde von den Aufsichtsbehörden aus Hessen, Mecklenburg-Vorpommern, Sachsen, Schleswig-Holstein und der Evangelischen Kirche Deutschlands zur Erprobung der SDM-Methode erarbeitet und veröffentlicht. Dieser Baustein ist keine Publikation der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder.

1. Bezug zu Gewährleistungszielen

Verfügbarkeit, Integrität, Intervenierbarkeit, Transparenz

2. Beschreibung

Personenbezogene Daten müssen gespeichert werden, um sie vom Zeitpunkt der Erhebung über die gesamte Dauer der rechtlich gebotenen Speicherpflichten bis zum Zeitpunkt der Aussonderung (Abgabe an Archive, Löschung oder Vernichtung) zur Verarbeitung bereitzustellen.

Speicherung umfasst das Erfassen, Aufnehmen und Aufbewahren von Daten. Betroffen sind einerseits Daten, die für den laufenden Bearbeitungsprozess ständig zur Verfügung stehen müssen (z. B. Patientendaten zur Erfüllung des mit Patienten abgeschlossenen Behandlungsvertrages während der medizinischen Behandlung im Krankenhaus oder Vertragsunterlagen zur Erfüllung handels- und steuerrechtlicher Anforderungen). Andererseits sind solche Daten betroffen, die für das tägliche Geschäft nicht mehr erforderlich sind, aufgrund rechtlich gebotener Speicherpflichten einschließlich Zwecken der Wahrung von Betroffenenrechten aber noch nicht gelöscht werden dürfen und die möglicher Weise auch außerhalb des Produktionssystems aufbewahrt werden (z. B. Patientendaten nach abgeschlossener medizinischer Behandlung, die u. a. zur Erfüllung der ärztlichen Dokumentationspflicht weiter aufbewahrt werden müssen oder Vertragsunterlagen, welche aus handels- und steuerrechtlichen Gründen auch nach Erfüllung des Vertrags aufbewahrt werden müssen). Damit sind Speicherfristen von wenigen Sekunden (z. B. automatisiertes Erfassen eines KfZ-Kennzeichens und sofortiges Löschen nach dem Abgleich mit einer Suchliste bei Nichttreffern) bis hin zu vielen Jahrzehnten (z. B. ärztliche Aufzeichnungen zu medizinischen Behandlungen) möglich.

Der Baustein „Aufbewahrung“ beschreibt nur diejenigen Maßnahmen zur Speicherung von personenbezogenen Daten in elektronischer oder in Papierform, die zur Aufbewahrung in physikalischen Speichermedien (Datenträgern) über längere Zeiträume (Langzeitspeichersystem) erforderlich sind, um auf sie während des gesamten Aufbewahrungszeitraums zugreifen zu können. Der Begriff Aufbewahrung wird in diesem Baustein für die langfristige Informationserhaltung von Datenobjekten mit Personenbezug verwendet. Nicht betrachtet wird

dagegen das Aufbewahren von Daten in Form von Datensicherungen, die mit dem Ziel gespeichert werden, Datenbestände bei Verlust wiederherstellen zu können (Backups).

Auch nicht betrachtet wird hier die Form der Archivierung von Unterlagen mit personenbezogenen Daten, bei der die Abgabe von Unterlagen an Archive gesondert gesetzlich geregelt ist. Sie umfasst die Bewertung archivreifer und die Übernahme archivwürdiger Unterlagen, deren Erschließung, dauerhafte Verwahrung und Erhaltung als Archivgut sowie die Bereitstellung der Unterlagen für die Benutzung. Mit der Archivierung geht die datenschutzrechtliche Verantwortung für die in den Unterlagen befindlichen personenbezogenen Daten vom bisher zuständigen Verantwortlichen auf den für das Archiv Verantwortlichen über. In der Informationstechnik wird der Datenbestand, der für den laufenden Verarbeitungsprozess nicht mehr ständig zur Verfügung stehen muss, häufig ebenfalls als „Archiv“ bezeichnet. Dieses Verständnis ist jedoch abzugrenzen von der hier beschriebenen Archivierung im juristischen Sinn.

Aufzubewahrende Daten zählen somit zum Produktivdatenbestand, auch wenn diese für den operativen Betrieb nicht mehr erforderlich sind. Sie müssen weiterhin im erforderlichen Umfang verarbeitet werden können. Dabei ist sicherzustellen, dass die Daten verfügbar bleiben, auch wenn sich zwischenzeitlich Hardware und Software oder Geschäftsprozesse ändern. Um einen Überblick über die aufzubewahrenden Daten zu bekommen, ist zunächst eine Inventur aller vorhandenen Daten-Formate erforderlich (M11.01). Eine anhaltende Verfügbarkeit kann durch folgende Maßnahmen sichergestellt werden:

a) Die Datenobjekte werden auf Papier ausgedruckt, welches dann auf herkömmliche Weise aufbewahrt wird (M11.06).

   Diese Herangehensweise bedeutet jedoch einen Rückschritt aus dem Paradigma der elektronischen Geschäftstätigkeit bzw. Verwaltungsarbeit. Sie ist langfristig nicht mit den Forderungen der E-Government-Gesetze von Bund und Ländern nach elektronischer Aktenführung und mit den Bestrebungen von Verwaltung und Wirtschaft nach effizienten, elektronischen Geschäftsprozessen vereinbar. Diese Methode kommt deshalb nur in Betracht, wenn Datenobjekte nicht in ihrer originären Form aufbewahrt werden müssen. Die Variante wird in Zukunft an Bedeutung verlieren, kann aber für kleine Datenvolumen und für einen zeitlich überschaubaren Übergangszeitraum zumindest in Betracht gezogen werden.

b) Die bei der erstmaligen Speicherung verwendeten Systeme (Hardware, Betriebssystem, Software-Werkzeuge) bzw. dazu kompatible Systeme (z. B. die letzte Softwareversion, die ein Dokumentenformat noch öffnen kann) müssen vorgehalten und für die Dauer der Aufbewahrung gepflegt werden (M11.07). Da der Aufwand bei einer steigenden Menge an vorzuhaltenden Systemen zunimmt, ist dieser Ansatz allenfalls als mittelfristige Übergangslösung zu empfehlen. Hilfreich können Emulations- oder Virtualisierungstechniken sein, die es erlauben, veraltete Betriebssysteme und An-

wendungssoftware auf moderner Hardware zu emulieren bzw. lauffähig zu halten (M11.15).

Falls solche veralteten Systeme vorgehalten werden, muss ergänzend geprüft werden, wie der zusätzlichen Gefährdung begegnet werden kann, die aus diesen Hard- und Softwarekomponenten resultiert, die in der Regel nicht mehr dem Stand der Technik entsprechen. Dabei ist zu bedenken, dass für solche Komponenten von den Herstellern regelhaft keine Sicherheitspatches mehr bereitgestellt werden. Daher gilt es u. a., Zugriffsmöglichkeiten insbesondere von außerhalb eines gesicherten Netzwerkes möglichst restriktiv zu handhaben bzw. vollständig zu unterbinden (M11.08).

c) Die Datenobjekte können mit Beginn der Aufbewahrung (und ggf. zusätzlich von Zeit zu Zeit währenddessen) in neue digitale Repräsentationen überführt werden (Transformation, Format-Migration – M11.09). Das neue Datenobjekt muss dabei ein vollwertiger Ersatz für das alte sein. Deshalb ist sicherzustellen, dass alle signifikanten Eigenschaften der Informationsobjekte erhalten und dass im Zuge des Überführens sämtliche Gewährleistungsziele eingehalten werden, also bspw. weder die Integrität der Daten noch die Zweckbindung oder Vertraulichkeit des Datenbestands gefährdet ist.

   Diese Variante ist 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 den Verantwortlichen oder den Auftragsverarbeiter im jeweils erforderlichen Umfang weiter verarbeitbar sind. Dadurch soll den Grundsätzen der Verfügbarkeit, Integrität und Intervenierbarkeit jederzeit genügt werden 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 alle Inhaltsdaten die Datenformate, die Syntax und die Semantik detailliert festgelegt und dokumentiert werden (M11.02). Bei der Wahl der Datenformate ist anzustreben, dass die Daten plattform- und herstellerunabhängig, eindeutig interpretierbar und für die Dauer der gesetzlichen Aufbewahrungsfristen in entsprechenden technischen Systemen 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.

Damit die Eigenschaften der Informationsobjekte auch nach der Überführung in neue digitale Repräsentationen erhalten bleiben, ist frühzeitig zu definieren, welches die „signifikanten Eigenschaften“ der im Langzeitspeicher abzulegenden Dokument-Typen, ihre zukünftige Ziel- oder Nutzergruppe sowie die Art der zukünftigen Verwendung sind (M11.03).

Neben den Inhaltsdaten sind Metadaten erforderlich, die einerseits helfen, die Ursprungsdaten aufzufinden und andererseits sicherstellen, dass aus Repräsentationen und ihren Daten für den Menschen interpretierbare Informationsobjekte wieder hergestellt werden. Das betrifft bspw.

- „beschreibende Metadaten“ wie Aktenzeichen, Betreff, Bezug oder Einsender,
- „technische Metadaten“ wie Dateiname, Dateiformat, Dateigröße, Hashwerte, in der Ausgangsdatei eingebettete Metadaten 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 den Zeitraum der Aufbewahrung muss festgelegt werden, welche Metadaten in welchen Formaten gemeinsam mit den Inhaltsdaten gespeichert werden (M11.04). Für eine langfristige Ablage der Metainformationen sind aktuell das XML-, das XSD- oder das JSON-Format geeignet.

In bestimmten Fällen ist der Beweiswert von Daten während des Zeitraums der Aufbewahrung zu erhalten (bspw. bei Dokumenten mit Urkundencharakter). Zu diesem Zweck sind Verifikationsdaten (elektronische Beweisdaten) erforderlich, die gemeinsam mit den Inhaltsdaten für den Zeitraum der Aufbewahrung gespeichert werden müssen (M11.05). Diese Daten müssen sämtliche Informationen enthalten, die zur Verifikation der Authentizität und Integrität der gespeicherten Daten, deren Signaturen, Zertifikate und der Signaturerneuerungen benötigt werden (siehe dazu auch Technische Richtlinie TR-03125 des BSI).

Systeme

Damit die eingesetzte Technik die datenschutzrechtlichen Anforderungen erfüllen kann, müssen die datenschutzrechtlichen Erfordernisse auf IT-Systemen abgebildet werden können. 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 so ausgestaltet werden, das sie unabhängig von einer bestimmten Software- und Hardware-Umgebung sind.

Die folgenden technischen Maßnahmen können dazu beitragen, eine dauerhafte physikalische Speicherung zu gewährleisten:

- redundante Vorhaltung der Datenbestände (M11.10)
- räumlich verteilte Speicherung der Daten (M11.11)
- parallele Nutzung unterschiedlicher Speichersysteme („Diversität“ - M11.12)
- regelmäßiges Ersetzen von Datenträgern („Refreshment“ - M11.13)
- regelmäßige Migration auf andere Speichersysteme („Replication“ - M11.14)
- Erhalten der Lauffähigkeit veralteter Software (Betriebssysteme, Anwendungssoftware) durch Virtualisierung oder Emulation (M11.15)
- Gewährleistung der Echtheit und Unverfälschtheit von Archivdatenobjekten beim Abruf von Nachweisen, indem die Middleware sämtliche hierfür erforderlichen elektronischen Beweisdaten erstellt und zurückgibt (M11.16)
- Protokollierungs-Systeme (M11.17)
- Sicherungs- und Rücksicherungs-Verfahren und -techniken („Recovery“ - M11.18)
- Umsetzung von Maßnahmen, mit denen gesetzlich geforderte Mandantentrennungen bei einer erneuten Nutzung der Daten gewährleistet werden (M11.19)
- Maßnahmen zum Erhalt der Beweiskraft der im Aufbewahrungsspeicher verbleibenden Dokumente beim Löschen anderer aufbewahrter Datenobjekte (M11.20)

Prozesse

Es sind organisatorische Prozesse erforderlich, die regeln, wer nach welchen Vorgaben und nach welchen rechtlichen Kriterien die Aufbewahrungsdauer festlegt. Bei Änderung der rechtlichen Rahmenbedingungen ist stets eine Anpassung bzw. Aktualisierung der organisatorischen Prozesse erforderlich. 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 (M11.22) und der Zeitpunkt der Konvertierung in das Aufbewahrungsformat bzw. der Migration auf andere Speichersysteme zu definieren (M11.23). Dafür benutzte Konvertierungstools dürfen nur integrationsgesichert eingesetzt werden. In diesem Zusammenhang sind auch Prozesse zu definieren, die den Umgang mit versionierten Daten steuern (M11.24).

Ein Dokumentationsprozess muss sicherstellen, dass auch bei langfristiger Aufbewahrung jederzeit nachvollzogen werden kann, welche Hard- und Software erforderlich ist, um die Daten verarbeiten zu können. Jede Formatkonvertierung und jede Migration auf andere Speichersysteme ist zu protokollieren (M11.25; M11.26). Dabei ist zu dokumentieren, ob und ggf. wie sich die Zieldaten von den Quelldaten unterscheiden (z. B. Reduzierung der Auflösung, Farbtiefe, Auslagerung von Meta-Informationen in ein Sidecar File[1]) und welche die Integrität gefährdenden, manipulierenden Operationen an den digitalen Objekten durchgeführt wurden (M11.27).

[1] Sidecar-Dateien (auch bekannt als Buddy-Dateien) sind Dateien, die Daten (oft Metadaten) in einem anderen Format als das der Quelldatei speichern. Sidecar-Dateien haben i. d. R. den gleichen Basisnamen wie die Quelldatei, aber mit einer anderen Erweiterung.

Es müssen technische und organisatorische Prozesse spezifiziert und implementiert werden, mit denen die Wiederherstellung von Daten binnen vorgegebener Fristen möglich ist (M11.28; M11.29). Dies ist Voraussetzung, um sowohl ein nachträgliches Ändern aufbewahrter Daten (Ändern, Löschen, Einschränken der Verarbeitung) – bspw. als Folge der Intervention Betroffener – als auch die Auskunft an Betroffene bezüglich ihrer gespeicherten Daten technisch und organisatorisch zu gewährleisten.

Sofern das Löschen von Daten und Dokumenten *vor* Ablauf des gesetzlich vorgeschriebenen Aufbewahrungszeitraums zulässig ist, muss dies durch organisatorisch berechtigte Nutzer einer technisch berechtigten vorgelagerten IT-Anwendung angestoßen und durch entsprechende Protokolle dokumentiert 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 (M11.21).

3. Differenzierung bei hohem Schutzbedarf

Es sind geeignete Maßnahmen vorzusehen und zu implementieren, die einerseits eine unzulässige Manipulation oder den unzulässigen Austausch von Komponenten oder Modulen und die unberechtigte Kenntnisnahme der Daten zuverlässig verhindern und andererseits die Integrität und Authentizität der Daten gewährleisten.

Zum einen ist in der Regel dann von hohem Schutzbedarf auszugehen, wenn der Beweiswert von Daten während des Zeitraums der Aufbewahrung erhalten werden muss (bspw. bei der elektronischen Speicherung von Urkunden oder Verwaltungsakten oder aufgrund gesetzlicher Vorschriften). Durch zusätzliche physische Sicherungsmaßnahmen (bspw. elektronische Signaturen) müssen die IT-Infrastruktur zur beweiswerterhaltenden Archivierung und die entsprechenden Speichermedien (M11.20) vor Verlust, Zerstörung sowie unberechtigter Veränderung geschützt werden, etwa durch Unterbringung der technischen Komponenten in zertifizierten Hochsicherheitsrechenzentren.

So gelten bspw. für die Führung der (elektronischen) Personenstandsregister Fristen von 80 Jahren für Eheregister und Lebenspartnerschaftsregister, von 110 Jahren für Geburtenregister und von 30 Jahren für Sterberegister. Daten dieser Register haben einen besonders hohen Schutzbedarf, da sie Eheschließung, Begründung der Lebenspartnerschaft, Geburt und Tod beweisen. Die Datenverarbeitungsverfahren für die Personenstandsregister (Registerverfahren) müssen daher u. a. gewährleisten, dass die Beurkundungsdaten als Personenstandseintrag auf Dauer unveränderbar gespeichert und dass die erforderliche dauerhaft überprüfbare qualifizierte elektronische Signatur und die Daten, die zur Sicherung der dauerhaften Überprüfbarkeit erforderlich sind, beim Personenstandseintrag gespeichert werden.

Zum anderen ist in der Regel auch dann hoher Schutzbedarf gegeben, wenn besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) verarbeitet werden. Dazu gehören bspw. Daten medizinischer Behandlungen (behandlungsbezogene Dokumente), die gemäß der Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren sind (§ 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.

Bei hohem Schutzbedarf hinsichtlich der Vertraulichkeit ist eine verschlüsselte Speicherung der Regelfall.

Bei hohem Schutzbedarf ist die Wirksamkeit der erforderlichen Maßnahmen einem besonders sorgfältigen Prüfprozess zu unterziehen. Beispielsweise sind an die Prozesse, die die Verfügbarkeit, Integrität und Vertraulichkeit der Daten nach einer Migration auf andere Speichersysteme prüfen, besonders hohe Anforderungen hinsichtlich ihrer ordnungsgemäßen Funktion zu stellen. Beim Einsatz von Virtualisierungs- und Emulationstechniken (M11.15) ist durch geeignete Mandantentrennungen sicherzustellen, dass die Nichtverkettung auch auf einem Hostsystem nicht unterlaufen wird. Zudem sind regelmäßige Tests auf Verfügbarkeit und Lesbarkeit angebracht. Die gewählte Aufbewahrungsstrategie sollte dokumentiert sein und die Speicherungsorte sollten ausdrücklich festgelegt sein.

4. Referenzen

IT-PLR: *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 31644:2012-04 (Kriterien für vertrauenswürdige digitale Langzeitarchive)*
DIN 31645:2011-11 (Leitfaden zur Informationsübernahme in digitale Langzeitarchive)
DIN 31647:2015-05 (Beweiswerterhaltung kryptographisch signierter Dokumente)

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

5. Zusammenfassung der Maßnahmen

Ebene Daten

M11.01 Inventur aller vorhandenen Daten-Formate vor der Aufbewahrung
M11.02 Festlegung geeigneter Datenformate für die aufzubewahrenden Daten
M11.03 Definition der signifikanten Eigenschaften der im Langzeitspeicher abzulegenden Dokument-Typen, ihrer zukünftige Ziel- oder Nutzergruppe sowie der Art der zukünftigen Verwendung
M11.04 Festlegung von Art, Umfang und Format der mit aufzubewahrenden Metadaten
M11.05 Festlegung aller Verifikationsdaten, die zum Erhalt des Beweiswertes von Daten mit aufbewahrt werden müssen

Ebene Systeme

M11.06 Ausdruck von aufzubewahrenden Daten auf Papier
M11.07 Aufbewahrung von Hard- und Softwarekomponenten für den Zeitraum der Aufbewahrung der damit ursprünglich verarbeiteten Daten
M11.08 Spezielle Zugriffsschutzmechanismen für Hard- und Softwarekomponenten, die nicht mehr dem Stand der Technik entsprechen
M11.09 Überführung aufzubewahrender Daten in neue digitale Repräsentationen
M11.10 Redundante Vorhaltung von Datenbeständen
M11.11 Räumlich verteilte Speicherung von Daten
M11.12 Parallele Nutzung unterschiedlicher Speichersysteme
M11.13 Regelmäßiges Ersetzen von Datenträgern (Refreshment)
M11.14 Regelmäßige Migration auf andere Speichersysteme
M11.15 Virtualisierungs- oder Emulationstechniken zum Erhalt der Lauffähigkeit veralteter Software
M11.16 Bereitstellung der erforderlichen elektronischen Beweisdaten durch die Middleware
M11.17 Protokollierungssysteme
M11.18 Backup- und Restore-Systeme für aufbewahrte Daten
M11.19 technische Systeme zur Realisierung von Mandantentrennungen
M11.20 Beweiswert erhaltende Speichertechniken

Ebene Prozesse

M11.21 Festlegung von Zuständigkeiten für alle Details der Aufbewahrung
M11.22 Definition der Kriterien für die Auswahl der technischen Systeme zur Erhaltung der Daten
M11.23 rechtzeitige Festlegung des Zeitpunktes der Konvertierung in das Aufbewahrungsformat bzw. der Migration auf andere Speichersysteme
M11.24 Regeln zum Umgang mit versionierten Daten

M11.25 Prozesse für die Protokollierung jeder Formatkonvertierung und für die Prüfung der Protokolle

M11.26 Prozesse für die Protokollierung jeder Migration auf andere Speichersysteme und für die Prüfung der Protokolle

M11.27 Dokumentation aller manipulierenden Operationen an den digitalen Objekten, die zur dauerhaften Aufbewahrung erforderlich sind

M11.28 Sicherungs- und Rücksicherungs-Strategien

M11.29 Prozess zur Prüfung der Einhaltung vorgegebener Fristen zur Wiederherstellung von Daten

6. Anmerkung zur Nutzung dieses Bausteins