CycleSEC®

Benutzerdefiniert

CON.2: Konzepte und Vorgehensweisen - Datenschutz

CON.2.bd.1 Generische Maßnahmen im SDM

1. Beschreibung

1.1 Einleitung

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat am 14. Mai 2024 mit der Version 3.1 eine überarbeitete Version des Standard-Datenschutzmodells (SDM) verabschiedet. Das SDM soll die rechtlichen Anforderungen der DS-GVO über die Gewährleistungsziele[1] in technische und organisatorische Maßnahmen (TOMs) überführen. Es soll so die Transformation abstrakter rechtlicher Anforderungen in konkrete technische und organisatorische Maßnahmen unterstützen.

Das Standard-Datenschutzmodell (SDM) führt in Abschnitt D1 generische technische und organisatorische Maßnahmen (TOMs) auf, „die in der Datenschutzprüfpraxis vieler Datenschutzaufsichtsbehörden seit vielen Jahren erprobt sind“. Zur Umsetzung dieser generischen TOMs in einem bestehenden ISMS nach BSI-Standards 200-1 und 200-2 müssen diese in einen benutzerdefinierten Baustein überführt werden.

Für eine weitere Einleitung in das Thema Standard-Datenschutzmodell (SDM) siehe Einleitung zu Baustein CON.2 *Datenschutz*.

1.2 Zielsetzung

Ziel des Bausteins ist es, die generischen Maßnahmen des Standard-Datenschutzmodells in einem benutzerdefinierten Baustein darzustellen und sie so in einem bestehenden ISMS modellierbar zu machen.

1.3 Abgrenzung und Modellierung

Der Baustein CON.2.bd.1 *Generische Maßnahmen im SDM* ist mindestens einmal für den Informationsverbund und ggf. für jede Verarbeitungstätigkeit anzuwenden, wenn personenbezogene Daten unter deutschem oder europäischem Recht verarbeitet werden.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein überführt die generischen Maßnahmen aus Abschnitt D1 im Standard-Datenschutzmodell (SDM) in benutzerdefinierte Anforderungen. Dabei lassen sich drei Fälle von resultierenden Anforderungen unterscheiden:

1. Die resultierende Anforderung enthält
    - Vorgaben zur Modellierung des Informationsverbunds mit einem oder mehreren Bausteinen des IT-Grundschutzkompendiums.

[1] Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

2. Die resultierende Anforderung enthält
    - Vorgaben zur Modellierung des Informationsverbunds mit einem oder mehreren Bausteinen des IT-Grundschutzkompendiums und
    - Vorgaben, die NICHT mit einem oder mehreren Bausteinen des IT-Grundschutzkompendiums modelliert werden können.
3. Die resultierende Anforderung enthält
    - Vorgaben, die NICHT mit einem oder mehreren Bausteinen des IT-Grundschutzkompendiums modelliert werden können.

Die Fälle 1. und 2. sind untypisch für einen (benutzerdefinierten) Baustein im IT-Grundschutz. Sie sind notwendig, um die vollständige Abdeckung der generischen Maßnahmen im Standard-Datenschutzmodell (SDM) im Baustein CON.2.bd.1 *Generische Maßnahmen im SDM* sichtbar und im IT-Grundschutz-Check prüfbar zu machen.

Dieser Baustein konkretisiert keine Anforderungen, die bereits in den Basis-Anforderungen der in CON.2.bd.1.A1 genannten Bausteine enthalten sind. Falls zur Erfüllung des Bausteins CON.2.bd.1 *Generische Maßnahmen im SDM* darüber hinaus Standard-Anforderungen bzw. Anforderungen bei erhöhtem Schutzbedarf aus Bausteinen des IT-Grundschutz-Kompendiums zu modellieren sind, wird in CON.2.bd.1.A2 und CON.2.bd.1.A3 explizit darauf hingewiesen.

Im Anhang ist dieser Zusammenhang zwischen den generischen technischen und organisatorischen Maßnahmen des SDM und den Anforderungen des Bausteins CON.2.bd.1 *Generische Maßnahmen im SDM* lückenlos nachvollziehbar.

Dieser Baustein behandelt ausschließlich die generischen technischen und organisatorischen Maßnahmen im Standard-Datenschutzmodell (SDM) Version 3.1.

Dieser Baustein behandelt **nicht** die Anforderungen der SDM-Bausteine des Referenzmaßnahmen-Katalogs des Standard-Datenschutzmodells (SDM).

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein CON.2.bd.1 *Generische Maßnahmen im SDM* von besonderer Bedeutung.

Es gilt die *Gefährdungslage* in Baustein CON.2 *Datenschutz.*

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.2.bd.1 *Generische Maßnahmen im SDM* aufgeführt. Die Institutionsleitung ist dafür verantwortlich, dass die datenschutzrechtlichen Bestimmungen eingehalten werden. Die Umsetzung der zur Sicherstellung des Datenschutzes erforderlichen Maßnahmen kann sie an eine Organisationseinheit delegieren. Hiervon abzugrenzen ist die Rolle der oder des Datenschutzbeauftragten. Zu ihren Aufgaben gemäß Artikel 39 DS-GVO gehört es, die Verantwortlichen, die Auftragsverarbeiter und deren jeweilige Mitarbeitende über ihre datenschutzrechtlichen Pflichten zu unterrichten und zu beraten. Ferner gehört es zu ihren Aufgaben, zu überwachen, ob die datenschutzrechtlichen Bestimmungen eingehalten werden. Die Verantwortung für die Wahrung des Datenschutzes verbleibt hingegen bei den Verantwortlichen bzw. den Auftragsverarbeitern. Der oder die Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der oder die ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Institutionsleitung
Weitere Zuständigkeiten	Datenschutzbeauftragte, Informationssicherheitsbeauftragte (ISB), Fachverantwortliche, IT-Betrieb

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]

Die Bausteine

- CON.1 *Kryptokonzept*
- CON.3 *Datensicherungskonzept*
- CON.6 *Löschen und Vernichten*
- CON.9 *Informationsaustausch*
- DER.3.1 *Audits und Revisionen*
- DER.4 *Notfallmanagement*
- ISMS.1 *Sicherheitsmanagement*
- OPS.1.1.1 *Allgemeiner IT-Betrieb*
- OPS.1.1.3 *Patch- und Änderungsmanagement*
- OPS.1.1.4 *Schutz vor Schadprogrammen*
- OPS.1.1.5 *Protokollierung*
- OPS.1.1.6 *Software-Tests und Freigaben*
- ORP.1 *Organisation*
- ORP.2 *Personal*
- ORP.4 *Identitäts- und Berechtigungsmanagement*

MÜSSEN einmal auf den gesamten Informationsverbund angewendet werden.

Der Baustein INF.1 *Allgemeines Gebäude* MUSS für jedes Gebäude einmal angewendet werden.

CON.2.bd.1.A2 Modellierung von Standard-Anforderungen (B) [Informationssicherheitsbeauftragte (ISB)]

Bei der Modellierung der Verarbeitungstätigkeiten MÜSSEN neben den Basis-Anforderungen gemäß CON.2.bd.1.A1 zusätzlich die folgenden Standard-Anforderungen angewendet werden:

- CON.1.A5 *Sicheres Löschen und Vernichten von kryptografischen Schlüsseln (S) [IT-Betrieb, Benutzende]*
- CON.1.A10 *Erstellung eines Kryptokonzepts (S)*
- CON.6.A8 *Erstellung einer Richtlinie für die Löschung und Vernichtung von Informationen (S) [Mitarbeitende, IT-Betrieb, Datenschutzbeauftragte]*
- CON.9.A8 *Verschlüsselung und digitale Signatur (S)*
- OPS.1.1.3.A5 *Umgang mit Änderungsanforderungen (S) [Fachverantwortliche]*
- OPS.1.1.3.A6 *Abstimmung von Änderungsanforderungen (S)*
- OPS.1.1.3.A7 *Integration des Änderungsmanagements in die Geschäftsprozesse (S)*

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

- OPS.1.1.5.A9 *Bereitstellung von Protokollierungsdaten für die Auswertung (S)*
- ORP.2.A7 *Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden (S)*
- ORP.4.A12 *Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen (S) [IT-Betrieb]*
- ORP.4.A13 *Geeignete Auswahl von Authentisierungsmechanismen (S) [IT-Betrieb]*
- ORP.4.A17 *Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen (S) [IT-Betrieb]*

Bei der Modellierung der Verarbeitungstätigkeiten MÜSSEN neben den Basis-Anforderungen aller im Informationsverbund modellierten Bausteine jeweils die Standard-Anforderungen angewendet werden,

- die eine Verschlüsselung fordern. Dies sind insbesondere:
  - APP.4.3.A16 *Verschlüsselung der Datenbankanbindung (S)*
  - INF.9.A9 *Verschlüsselung tragbarer IT-Systeme und Datenträger (S) [IT-Betrieb]*
  - NET.4.2.A8 *Verschlüsselung von VoIP (S)*
  - SYS.3.1.A13 *Verschlüsselung von Laptops (S)*
  - SYS.3.2.1.A11 *Verschlüsselung des Speichers (S)*
  - SYS.4.1.A15 *Verschlüsselung von Informationen bei Druckern, Kopierern und Multifunktionsgeräten (S)*
- die eine Auswertung von Protokollen fordern. Dies sind insbesondere:
  - APP.3.6.A15 *Auswertung der Logdaten (S)*
  - DER.1.A6 *Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten (S)*
- die eine Härtung fordern. Dies sind insbesondere:
  - INF.13.A11 *Angemessene Härtung von Systemen im TGM (S)*
  - SYS.1.9.A15 *Härtung des Terminalservers (S)*
  - SYS.2.5.A8 *Härtung der virtuellen Clients (S)*
  - SYS.2.6.A7 *Härtung der virtualisierten Clients durch die VDI-Lösung (S)*
  - SYS.2.6.A8 *Härtung der VDI-Lösung (S)*

CON.2.bd.1.A3 Modellierung von Anforderungen für erhöhten Schutzbedarf (B) [Informationssicherheitsbeauftragte (ISB)]

Bei der Modellierung der Verarbeitungstätigkeiten MÜSSEN neben den Basis-Anforderungen aller im Informationsverbund modellierten Bausteine jeweils die Anforderungen für erhöhten Schutzbedarf angewendet werden,

- die eine Verschlüsselung fordern. Dies sind insbesondere:
  - APP.3.3.A12 *Verschlüsselung des Datenbestandes (H)*
  - NET.4.2.A14 *Verschlüsselung der Signalisierung (H)*
  - OPS.1.1.5.A12 *Verschlüsselung der Protokollierungsdaten (H)*
  - OPS.2.2.A17 *Einsatz von Verschlüsselung bei Cloud-Nutzung (H)*
  - SYS.1.5.A28 *Verschlüsselung von virtuellen IT-Systemen (H)*
  - SYS.1.8.A23 *Einsatz von Verschlüsselung für Speicherlösungen (H)*
  - SYS.1.9.A17 *Verschlüsselung der Übertragung (H)*
  - SYS.2.1.A28 *Verschlüsselung der Clients (H)*
- die eine Auswertung von Protokollen fordern. Dies ist insbesondere:
  - DER.1.A14 *Auswertung der Protokollierungsdaten durch spezialisiertes Personal (H)*
- die eine Härtung fordern. Dies sind insbesondere:
  - SYS.1.1.A38 *Härtung des Host-Systems mittels Read-Only-Dateisystem (H)*
  - OPS.1.1.4.A14 *Auswahl und Einsatz von Cyber-Sicherheitsprodukten gegen gezielte Angriffe (H)*
  - SYS.1.5.A22 *Härtung des Virtualisierungsservers (H)*

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

CON.2.bd.1.A4 Dokumentation der Daten-Syntax (B) [Fachverantwortliche]

Für jede Verarbeitungstätigkeit MUSS der Syntax von personenbezogenen Daten dokumentiert werden. Dazu SOLLTEN entsprechende Regelungen erarbeitet werden.

CON.2.bd.1.A5 Gewährleistung der Redundanz von Hard- und Software sowie Infrastruktur (B) [IT-Betrieb]

Verarbeitungstätigkeiten MÜSSEN gegen Ausfälle in geeigneter Weise geschützt sein. Hierzu MÜSSEN mindestens geeignete Redundanzen verfügbar sein und es SOLLTEN Wartungsverträge mit den Lieferanten abgeschlossen werden.

CON.2.bd.1.A6 Berücksichtigung von datenschutzrechtlichen Anforderungen im Kryptokonzept (B) [Informationssicherheitsbeauftragte (ISB)]

Verarbeitungstätigkeiten MÜSSEN durch Prüfsummen, elektronische Siegel und Signaturen geschützt werden. Die hierfür nötigen Anforderungen MÜSSEN im Kryptokonzept festgelegt werden.

CON.2.bd.1.A7 Sicherstellung der Richtigkeit von Daten (B) [Fachverantwortliche]

Personenbezogene Daten MÜSSEN unverzüglich berichtigt werden, sobald die Institution Kenntnis von Fehlern in den Daten erfährt.

Es MÜSSEN Prozesse existieren, um die Aktualität von Daten zu gewährleisten.

CON.2.bd.1.A8 Testen von Verarbeitungstätigkeiten (B) [Fachverantwortliche]

Tests von Verarbeitungstätigkeiten MÜSSEN für die Feststellung

- der korrekten Funktionalität,
- von Risiken
- sowie Sicherheitslücken
- und Nebenwirkungen

von Prozessen geeignet sein.

Die Ergebnisse von Tests MÜSSEN dokumentiert werden.

CON.2.bd.1.A9 Berücksichtigung von datenschutzrechtlichen Anforderungen im Berechtigungs- und Rollenkonzept (B) [Fachverantwortliche]

Bei der Festlegung des Berechtigungs- und Rollenkonzeptes MUSS das Erforderlichkeitsprinzip eingehalten werden.

CON.2.bd.1.A10 Bestimmung von Interessenskonflikten (B) [Fachverantwortliche]

Die Institution MUSS unvereinbare Aufgaben und Funktionen (Interessenskonflikte) für die Verarbeitungstätigkeit definieren (siehe ORP.4.A4 *Aufgabenverteilung und Funktionstrennung*).

CON.2.bd.1.A11 Freigabe und Kontrolle von zugelassenen Ressourcen für Verarbeitungstätigkeiten (B) [Informationssicherheitsbeauftragte (ISB)]

Für jede Verarbeitungstätigkeit MÜSSEN zugelassene Ressourcen freigegeben werden. Hierzu gehören insbesondere:

- IT-System
- Kommunikationskanäle
- spezifische Gebäude und/oder Räume, die für die Verarbeitungstätigkeit ausgestattet sind.

Die Nutzung der freigegebenen Ressourcen im Rahmen der Freigabe MUSS angemessen kontrolliert werden.

CON.2.bd.1.A12 Abschluss von Vertraulichkeitsvereinbarungen und Verpflichtungen auf das Datengeheimnis (B) [Informationssicherheitsbeauftragte (ISB), Fachverantwortliche]

Bevor Personen Zugang und Zugriff zu personenbezogenen Daten erhalten, MÜSSEN

- mit ihnen schriftliche Vertraulichkeitsvereinbarungen geschlossen werden,

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

- sie schriftlich auf das Datengeheimnis verpflichtet werden.

CON.2.bd.1.A13 Beschränkung von Verarbeitungstätigkeiten (B) [Fachverantwortliche]

Für Verarbeitungstätigkeiten MÜSSEN Verarbeitungs-, Nutzungs- und Übermittlungsrechte auf das notwendige Minimum beschränkt werden.

Für Verarbeitungstätigkeiten DÜRFEN KEINE Schnittstellen aktiviert oder entwickelt werden, die nicht dem rechtmäßigen Zweck dienen.

Verarbeitungstätigkeiten DÜRFEN KEINE Backdoors enthalten. Das Verbot MUSS schriftlich dokumentiert werden. Die Einhaltung des Verbots im Rahmen der Softwareentwicklung MUSS sichergestellt werden.

CON.2.bd.1.A14 Pseudonymisierung und Anonymisierung von Daten (B) [Fachverantwortliche, IT-Betrieb]

Verarbeitungstätigkeiten MÜSSEN so gestaltet sein, dass möglichst Pseudonyme, Anonymisierungsdienste, anonyme Credentials und pseudonymisierte oder anonymisierte Daten verwendet werden.

CON.2.bd.1.A15 Zusätzliche Dokumentation bei Verarbeitungstätigkeiten (B) [Fachverantwortliche, IT-Betrieb]

Es MUSS ein Verzeichnis der Verarbeitungstätigkeiten (VVT) gemäß Art. 30 DS-GVO angelegt werden. Das Verzeichnis der Verarbeitungstätigkeiten (VVT) MUSS die folgenden Angaben enthalten:

- Geschäftsprozesse
- Datenbestände
- Datenflüsse
- Netzpläne
- genutzte IT-Systeme
- Betriebsabläufe
- Beschreibungen von Verarbeitungstätigkeiten
- Zusammenspiel mit anderen Verarbeitungstätigkeiten

Die folgenden Informationen MÜSSEN dokumentiert werden:

- Quelle von Daten
- Art der Umsetzung der Informationspflichten gegenüber Betroffenen
- wo deren Daten erhoben wurden
- Umgangs mit Datenpannen
- Faktoren, die für eine Profilierung, zum Scoring oder für teilautomatisierte Entscheidungen genutzt werden
- Verträge mit Personen und Organisationen, von denen Daten erhoben bzw. an die Daten übermittelt werden
- Einwilligungen zu einer Verarbeitung, deren Widerruf sowie Widersprüche

Falls die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, MUSS eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden.

CON.2.bd.1.A16 Sicherstellung einer Versionierung und Änderungsverfolgung (B) [Fachverantwortliche, IT-Betrieb]

Verarbeitungstätigkeiten MÜSSEN so gestaltet sein, dass eine Versionierung und Änderungsverfolgung ermöglicht wird.

CON.2.bd.1.A17 Information und Benachrichtigung von Betroffenen (B) [Fachverantwortliche, Informationssicherheitsbeauftragte (ISB), Datenschutzbeauftragte]

Betroffenen MÜSSEN Informationen über die Verarbeitung von personenbezogenen Daten bereitgestellt werden.

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

Betroffene MÜSSEN bei Datenpannen oder bei Weiterverarbeitungen zu einem anderen Zweck benachrichtigt werden.

CON.2.bd.1.A18 Nachverfolgung der Aktivitäten der verantwortlichen Stelle zur Gewährung von Betroffenenrechten (B) [Institutionsleitung, Fachverantwortliche]

Die Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte MÜSSEN nachverfolgbar sein.

CON.2.bd.1.A19 Berücksichtigung von datenschutzrechtlichen Anforderungen im Protokollierungs- und Auswertungskonzept B) [Informationssicherheitsbeauftragte (ISB)]

Auskunftsrechte von Betroffenen MÜSSEN im Protokollierungs- und Auswertungskonzept berücksichtigt werden.

CON.2.bd.1.A20 Etablieren von Verfahren zu Einwilligungen zu einer Verarbeitung, deren Widerruf sowie Widersprüchen (B) [Institutionsleitung, Fachverantwortliche]

Verfahren zu einer differenzierten Einwilligung zu einer Verarbeitung, deren Widerruf sowie Verfahren für Widersprüche MÜSSEN vorhanden sein.

CON.2.bd.1.A21 Bereitstellung von Datenfeldern (B) [Fachverantwortliche, IT-Betrieb]

Die Verarbeitungstätigkeit MUSS insbesondere die folgenden Datenfelder enthalten:

- Sperrkennzeichen
- Benachrichtigungen
- Einwilligungen
- Widersprüche
- Gegendarstellungen

CON.2.bd.1.A22 Umsetzung einer datenschutzkonformen Systemarchitektur (B) [Institutionsleitung, Fachverantwortliche, IT-Betrieb]

Die Verarbeitungstätigkeit MUSS

- eine Deaktivierungsmöglichkeit einzelner Funktionalitäten bieten, ohne das Gesamtsystem in Mitleidenschaft zu ziehen,
- standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen besitzen,
- eine Schnittstelle für strukturierte, maschinenlesbare Daten zum Abruf durch Betroffene besitzen,
- operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten bereitstellen,
- so voreingestellt sein, dass die Verarbeitung von Daten auf das für den spezifischen Verarbeitungszweck erforderliche Maß beschränkt ist.

Für die Verarbeitungstätigkeit MÜSSEN Datenfelder

- maskiert werden, falls ihre vollständige oder teilweise Anzeige für den spezifischen Verarbeitungszweck unnötig ist,
- mit automatischen Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren ausgestattet werden, falls ihre dauerhafte Verarbeitung ohne diese Maßnahmen für den spezifischen Verarbeitungszweck unnötig ist.

Die Verarbeitungstätigkeit SOLLTE so entwickelt und konfiguriert sein, dass automatisierte Verarbeitungsprozesse (nicht Entscheidungsprozesse), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen bevorzugt werden.

CON.2.bd.1.A23 Umsetzung von institutionellen Vorgaben (B) [Institutionsleitung, Fachverantwortliche]

Die Institution MUSS

- Personen, die Betroffenenrechte wahrnehmen möchten identifizieren und authentifizieren,
- einen Single Point of Contact (SPoC) für Betroffene einrichten,

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

- Optionen für Betroffene bereitstellen, um Programme datenschutzgerecht einstellen zu können.

CON.2.bd.1.A24 Reduzierung datenschutzrelevanter Informationen und Vorgänge (B) [Institutionsleitung, Fachverantwortliche, IT-Betrieb]

Die Verarbeitungstätigkeit DARF KEINE für den spezifischen Verarbeitungszweck unnötigen

- Attribute zu betroffenen Personen erfassen
- Verarbeitungsoptionen in Verarbeitungsprozessschritten enthalten,
- Möglichkeiten der Kenntnisnahme vorhandener Daten bereitstellen.

3.2 Standard-Anforderungen

Für diesen Baustein sind keine Standard-Anforderungen definiert.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

CON.2.bd.1.A25 Modellierung von Anforderungen für erhöhten Schutzbedarf (H) [Informationssicherheitsbeauftragte (ISB)]

Bei der Modellierung der Verarbeitungstätigkeiten SOLLTE neben den Basis-Anforderungen gemäß CON.2.bd.1.A1 zusätzlich die folgende Anforderung für erhöhten Schutzbedarf angewendet werden:

- ORP.2.A13 *Sicherheitsüberprüfung (H)*

4. Weiterführenden Informationen

Für den Baustein CON.2.bd.1 *Generische Maßnahmen im SDM* werden die folgenden weiterführenden Informationen empfohlen:

1. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Herausgeber: AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder), Das Standard-Datenschutzmodell: Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 3.1 von der 107. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 14. Mai 2024 beschlossen

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

5. Anhang

Im Folgenden wird der Zusammenhang der generischen Maßnahmen mit den Anforderungen des Bausteins CON.2.bd.1 *Generische Maßnahmen im SDM* dargestellt.

Für den Inhalt der Spalte *Bezeichnung im SDM V.3.1* gilt der folgende Quellenvermerk: „Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz).“

5.1 D.1.1 Verfügbarkeit

Typische Maßnahmen zur Gewährleistung der Verfügbarkeit gemäß SDM sind:

Nummer im SDM	Bezeichnung im SDM V.3.1	Modellierung durch eine neue benutzerdefinierte Anforderung	Modellierung durch Baustein(e) des IT-Grundschutz-Kompendiums	Anforderung in CON.2.bd.1 *Generische Maßnahmen im SDM*
D.1.1 Aufz. 1	Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß einem getesteten Konzept (B1.20 Wiederherstellbarkeit)		Der Baustein CON.3 *Datensicherungskonzept* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.1 Aufz. 2	Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt) (B1.18 Verfügbarkeit, B1.19 Belastbarkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen)		Die Bausteine • ISMS.1 *Sicherheitsmanagement* • OPS.1.1.1 *Allgemeiner IT-Betrieb* • OPS.1.1.4 *Schutz vor Schadprogrammen* MÜSSEN einmal auf den gesamten Informationsverbund angewendet werden. Der Baustein INF.1 *Allgemeines Gebäude* MUSS für jedes Gebäude einmal angewendet werden.	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.1 Aufz. 3	Dokumentation der Syntax der Daten (B1.18 Verfügbarkeit, B1.20 Wiederherstellbarkeit)	Für jede Verarbeitungstätigkeit MUSS der Syntax von personenbezogenen Daten dokumentiert werden. Dazu SOLLTEN entsprechende Regelungen erarbeitet werden.		CON.2.bd.1.A4 Dokumentation der Daten-Syntax (B) [Fachverantwortliche]
D.1.1. Aufz. 4	Redundanz von Hard- und Software sowie Infrastruktur (B1.20 Verfügbarkeit, B1.19 Belastbarkeit)	Verarbeitungstätigkeiten MÜSSEN gegen Ausfälle in geeigneter Weise geschützt sein. Hierzu MÜSSEN mindestens geeignete Redundanzen verfügbar sein und es SOLLTEN Wartungsverträge mit den Lieferanten abgeschlossen werden.		CON.2.bd.1.A5 Gewährleistung der Redundanz von Hard- und Software sowie Infrastruktur (B) [IT-Betrieb]
D.1.1 Aufz. 5	Umsetzung von Reparaturstrategien und Ausweichprozessen (B1.19 Belastbarkeit, B1.20 Wiederherstellbarkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen)		Der Baustein DER.4 *Notfallmanagement* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

Nummer im SDM	Bezeichnung im SDM V.3.1	Modellierung durch eine neue benutzerdefinierte Anforderung	Modellierung durch Baustein(e) des IT-Grundschutz-Kompendiums	Anforderung in CON.2.bd.1 *Generische Maßnahmen im SDM*
D.1.1 Aufz. 6	Erstellung eines Notfallkonzepts zur Wiederherstellung einer Verarbeitungstätigkeit (B1.19 Belastbarkeit, B1.20 Wiederherstellbarkeit)		Der Baustein DER.4 *Notfallmanagement* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.1 Aufz. 7	Vertretungsregelungen für abwesende Mitarbeitende (B1.18 Verfügbarkeit)		Der Baustein ORP.2 *Personal* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]

5.2 D.1.2 Integrität

Typische Maßnahmen zur Gewährleistung der Integrität oder zur Feststellung von Integritätsverletzungen gemäß SDM sind:

Nummer im SDM	Bezeichnung im SDM V.3.1	Modellierung durch eine neue benutzerdefinierte Anforderung	Modellierung durch Baustein(e) des IT-Grundschutz-Kompendiums	Anforderung in CON.2.bd.1 *Generische Maßnahmen im SDM*
D.1.2 Aufz. 1	Einschränkung von Schreib- und Änderungsrechten (B1.6 Integrität)		Der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.2 Aufz. 2	Einsatz von Prüfsummen, elektronischen Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptokonzepts (B1.6 Integrität, B1.4 Richtigkeit, B1.23 Angemessene Überwachung der Verarbeitung, B1.22 Behebung und Abmilderung von Datenschutzverletzungen)	Verarbeitungstätigkeiten MÜSSEN durch Prüfsummen, elektronische Siegel und Signaturen geschützt werden. Die hierfür nötigen Anforderungen MÜSSEN im Kryptokonzept festgelegt werden.	Der Baustein CON.1 *Kryptokonzept* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A6 Berücksichtigung von datenschutzrechtlichen Anforderungen im Kryptokonzept (B) [Informationssicherheitsbeauftragte (ISB)] CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.2 Aufz. 3	Dokumentierte Zuweisung von Berechtigungen und Rollen (B1.6 Integrität)		Der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.2 Aufz. 4	Löschen oder Berichtigen falscher Daten (B1.4 Richtigkeit)	Personenbezogene Daten MÜSSEN unverzüglich berichtigt werden, sobald die Institution Kenntnis von Fehlern in den Daten erfährt.	Der Baustein CON.6 *Löschen und Vernichten* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A7 Sicherstellung der Richtigkeit von Daten (B) [Fachverantwortliche] CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.2 Aufz. 5	Härten von IT-Systemen, so dass diese keine oder möglichst wenige Nebenfunktionalitäten aufweisen (B1.6 Integrität, B1.19 Belastbarkeit)		Bei der Modellierung einer Verarbeitungstätigkeit MÜSSEN neben den Basis-Anforderungen aller im Informationsverbund modellierten Bausteine jeweils die Anforderungen der Standard-Anforderungen bzw. der Anforderungen für erhöhten Schutzbedarf angewendet werden die eine Härtung fordern. Dies sind insbesondere: • INF.13.A11 *Angemessene Härtung von Systemen im TGM (S)*	CON.2.bd.1.A2 Modellierung von Standard-Anforderungen (B) [Informationssicherheitsbeauftragte (ISB)] CON.2.bd.1.A3 Modellierung von Anforderungen für erhöhten Schutzbedarf (B) [Informationssicherheitsbeauftragte (ISB)]

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

Nummer im SDM	Bezeichnung im SDM V.3.1	Modellierung durch eine neue benutzerdefinierte Anforderung	Modellierung durch Baustein(e) des IT-Grundschutz-Kompendiums	Anforderung in CON.2.bd.1 *Generische Maßnahmen im SDM*
			• OPS.1.1.4.A14 *Auswahl und Einsatz von Cyber-Sicherheitsprodukten gegen gezielte Angriffe (H)* • SYS.1.1.A38 *Härtung des Host-Systems mittels Read-Only-Dateisystem (H)* • SYS.1.5.A22 *Härtung des Virtualisierungsservers (H)* • SYS.1.9.A15 *Härtung des Terminalservers (S)* • SYS.2.5.A8 *Härtung der virtuellen Clients (S)* • SYS.2.6.A7 *Härtung der virtualisierten Clients durch die VDI-Lösung (S)* • SYS.2.6.A8 *Härtung der VDI-Lösung (S)*	
D.1.2 Aufz. 6	Prozesse zur Aufrechterhaltung der Aktualität von Daten (B1.4 Richtigkeit)	Es MÜSSEN Prozesse existieren, um die Aktualität von Daten zu gewährleisten.		CON.2.bd.1.A7 Sicherstellung der Richtigkeit von Daten (B) [Fachverantwortliche]
D.1.2 Aufz. 7	Prozesse zur Identifizierung und Authentifizierung von Personen und Gerätschaften (B1.6 Integrität)		Der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.2 Aufz. 8	Festlegung des Sollverhaltens von Prozessen und regelmäßiger Durchführung von Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen (B1.6 Integrität, B1.16 Fehler- und Diskriminierungsfreiheit beim Profiling, B1.19 Belastbarkeit)	Tests von Verarbeitungstätigkeiten MÜSSEN für die Feststellung • der korrekten Funktionalität, • von Risiken • sowie Sicherheitslücken • und von Nebenwirkungen von Prozessen geeignet sein. Die Ergebnisse von Tests MÜSSEN dokumentiert werden.	Der Baustein OPS.1.1.6 *Software-Tests und Freigaben* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A8 Testen von Verarbeitungstätigkeiten (B) [Fachverantwortliche] CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.2 Aufz. 9	Festlegung des Sollverhaltens von Abläufen bzw. Prozessen und regelmäßiger Durchführung von Tests zur Feststellbarkeit bzw. Feststellung der Ist-Zustände von Prozessen (B1.6 Integrität, B1.16 Fehler- und Diskriminierungsfreiheit beim Profiling, B1.23 Angemessene Überwachung der Verarbeitung, B1.19 Belastbarkeit)		Der Baustein OPS.1.1.6 *Software-Tests und Freigaben* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.2 Aufz. 10	Schutz vor äußeren Einflüssen (Spionage, Hacking) (B1.6 Integrität, B1.19 Belastbarkeit,		Die Bausteine	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

Nummer im SDM	Bezeichnung im SDM V.3.1	Modellierung durch eine neue benutzerdefinierte Anforderung	Modellierung durch Baustein(e) des IT-Grundschutz-Kompendiums	Anforderung in CON.2.bd.1 *Generische Maßnahmen im SDM*
	B1.22 Behebung und Abmilderung von Datenschutzverletzungen)		• ISMS.1 *Sicherheitsmanagement* • OPS.1.1.1 *Allgemeiner IT-Betrieb* • OPS.1.1.3 *Patch- und Änderungsmanagement* MÜSSEN einmal auf den gesamten Informationsverbund angewendet werden. Bei der Modellierung einer Verarbeitungstätigkeit SOLLTE neben den Basis-Anforderungen zusätzlich die folgende Anforderung für erhöhten Schutzbedarf angewendet werden: • OPS.1.1.4.A14 *Auswahl und Einsatz von Cyber-Sicherheitsprodukten gegen gezielte Angriffe (H)*	CON.2.bd.1.A3 Modellierung von Anforderungen für erhöhten Schutzbedarf (B) [Informationssicherheitsbeauftragte (ISB)]

5.3 D.1.3 Vertraulichkeit

Typische Maßnahmen zur Gewährleistung der Vertraulichkeit gemäß SDM sind:

Nummer im SDM	Bezeichnung im SDM V.3.1	Modellierung durch eine neue benutzerdefinierte Anforderung	Modellierung durch Baustein(e) des IT-Grundschutz-Kompendiums	Anforderung in CON.2.bd.1 *Generische Maßnahmen im SDM*
D.1.3 Aufz. 1	Festlegung eines Berechtigungs- und Rollenkonzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle (B1.7 Vertraulichkeit)	Bei der Festlegung des Berechtigungs- und Rollenkonzeptes MUSS das Erforderlichkeitsprinzip eingehalten werden.	Die Bausteine • ORP.1 *Organisation* • ORP.4 *Identitäts- und Berechtigungsmanagement* MÜSSEN einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A9 Berücksichtigung von datenschutzrechtlichen Anforderungen im Berechtigungs- und Rollenkonzept (B) [Fachverantwortliche, Informationssicherheitsbeauftragte (ISB)] CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.3 Aufz. 2	Implementierung eines sicheren Authentifizierungsverfahrens (B1.7 Vertraulichkeit)		Der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.3 Aufz. 3	Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal zugelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen (B1.7 Vertraulichkeit)	Die Institution MUSS unvereinbare Aufgaben und Funktionen (Interessenskonflikte) für die Verarbeitungstätigkeit definieren (siehe ORP.4.A4 *Aufgabenverteilung und Funktionstrennung*).	Die Bausteine • ORP.1 *Organisation* • ORP.2 *Personal* • ORP.4 *Identitäts- und Berechtigungsmanagement* MÜSSEN einmal auf den gesamten Informationsverbund angewendet werden. Bei der Modellierung einer Verarbeitungstätigkeit MUSS neben den Basis-Anforderungen zusätzlich	CON.2.bd.1.A10 Bestimmung von Interessenskonflikten (B) [Fachverantwortliche] CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)] CON.2.bd.1.A2 Modellierung von Standard-Anforderungen (B) [Informationssicherheitsbeauftragte (ISB)] CON.2.bd.1.A25 Modellierung von Anforderungen für erhöhten Schutzbedarf (H) [Informationssicherheitsbeauftragte (ISB)]

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

			die folgende Standard-Anforderung angewendet werden: • ORP.2.A7 *Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden (S)* Bei der Modellierung einer Verarbeitungstätigkeit SOLLTE neben den Basis-Anforderungen zusätzlich die folgende Anforderung für erhöhten Schutzbedarf angewendet werden: • ORP.2.A13 *Sicherheitsüberprüfung (H)*	
D.1.3 Aufz. 4	Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle (B1.7 Vertraulichkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen)	Für jede Verarbeitungstätigkeit MÜSSEN zugelassene Ressourcen freigegeben werden. Hierzu gehören insbesondere: • … • Kommunikationskanäle • … Die Nutzung der freigegebenen Ressourcen im Rahmen der Freigabe MUSS angemessen kontrolliert werden.		CON.2.bd.1.A11 Freigabe und Kontrolle von zugelassenen Ressourcen für Verarbeitungstätigkeiten (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.3 Aufz. 5	Spezifizierte, für die Verarbeitungstätigkeit ausgestattete Umgebungen (Gebäude, Räume) (B1.7 Vertraulichkeit)	Für jede Verarbeitungstätigkeit MÜSSEN zugelassene Ressourcen freigegeben werden. Hierzu gehören insbesondere: • … • spezifische Gebäude und/oder Räume, die für die Verarbeitungstätigkeit ausgestattet sind.		CON.2.bd.1.A11 Freigabe und Kontrolle von zugelassenen Ressourcen für Verarbeitungstätigkeiten (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.3 Aufz. 6	Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen usw.) (B1.7 Vertraulichkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen)	Bevor Personen Zugang und Zugriff zu personenbezogenen Daten erhalten, MÜSSEN • mit ihnen schriftliche Vertraulichkeitsvereinbarungen geschlossen werden, • sie schriftlich auf das Datengeheimnis verpflichtet werden.	Die Bausteine • ISMS.1 *Sicherheitsmanagement* • DER.3.1 *Audits und Revisionen* • ORP.1 *Organisation* MÜSSEN einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A12 Abschluss von Vertraulichkeitsvereinbarungen und Verpflichtungen auf das Datengeheimnis (B) [Informationssicherheitsbeauftragte (ISB), Fachverantwortliche] CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.3 Aufz. 7	Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept) (B1.7 Vertraulichkeit)		Die Bausteine • CON.1 *Kryptokonzept* • CON.9 *Informationsaustausch* MÜSSEN einmal auf den gesamten Informationsverbund angewendet werden. Bei der Modellierung einer Verarbeitungstätigkeit MÜSSEN neben den Basis-Anforderungen zusätzlich die folgenden Standard-Anforderungen angewendet werden:	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)] CON.2.bd.1.A2 Modellierung von Standard-Anforderungen (B) [Informationssicherheitsbeauftragte (ISB)] CON.2.bd.1.A3 Modellierung von Anforderungen für erhöhten Schutzbedarf (B) [Informationssicherheitsbeauftragte (ISB)]

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

			• CON.1.A5 *Sicheres Löschen und Vernichten von kryptografischen Schlüsseln (S) [IT-Betrieb, Benutzende]* • CON.1.A10 *Erstellung eines Kryptokonzepts (S)* • CON.9.A8 *Verschlüsselung und digitale Signatur (S)* Bei der Modellierung einer Verarbeitungstätigkeit MÜSSEN neben den Basis-Anforderungen aller modellierten Bausteine jeweils die Standard-Anforderungen bzw. die Anforderungen für erhöhten Schutzbedarf angewendet werden, die eine Verschlüsselung fordern, falls ein vergleichbarer und angemessener Schutz nicht anders gewährleistet werden kann. Dies sind insbesondere: • APP.3.3.A12 *Verschlüsselung des Datenbestandes (H)* • APP.4.3.A16 *Verschlüsselung der Datenbankanbindung (S)* • INF.9.A9 *Verschlüsselung tragbarer IT-Systeme und Datenträger (S) [IT-Betrieb]* • NET.4.2.A8 *Verschlüsselung von VoIP (S)* • NET.4.2.A14 *Verschlüsselung der Signalisierung (H)* • OPS.1.1.5.A12 *Verschlüsselung der Protokollierungsdaten (H)* • OPS.2.2.A17 *Einsatz von Verschlüsselung bei Cloud-Nutzung (H)* • SYS.1.5.A28 *Verschlüsselung von virtuellen IT-Systemen (H)* • SYS.1.8.A23 *Einsatz von Verschlüsselung für Speicherlösungen (H)* • SYS.1.9.A17 *Verschlüsselung der Übertragung (H)* • SYS.2.1.A28 *Verschlüsselung der Clients (H)* • SYS.3.1.A13 *Verschlüsselung von Laptops (S)* • SYS.3.2.1.A11 *Verschlüsselung des Speichers (S)*	

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

			• SYS.4.1.A15 Verschlüsselung von Informationen bei Druckern, Kopierern und Multifunktionsgeräten (S)	
D.1.3 Aufz. 8	Schutz vor äußeren Einflüssen (Spionage, Hacking) (B1.7 Vertraulichkeit, Belastbarkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen)		Die Bausteine • ISMS.1 *Sicherheitsmanagement* • OPS.1.1.1 *Allgemeiner IT-Betrieb* • OPS.1.1.3 *Patch- und Änderungsmanagement* MÜSSEN einmal auf den gesamten Informationsverbund angewendet werden. Bei der Modellierung einer Verarbeitungstätigkeit SOLLTE neben den Basis-Anforderungen zusätzlich die folgende Anforderung für erhöhten Schutzbedarf angewendet werden: • OPS.1.1.4.A14 *Auswahl und Einsatz von Cyber-Sicherheitsprodukten gegen gezielte Angriffe (H)*	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)] CON.2.bd.1.A3 Modellierung von Anforderungen für erhöhten Schutzbedarf (B) [Informationssicherheitsbeauftragte (ISB)]

5.4 D.1.4 Nichtverkettung

Typische Maßnahmen zur Gewährleistung der Nichtverkettung gemäß SDM sind:

Nummer im SDM	Bezeichnung im SDM V.3.1	Modellierung durch eine neue benutzerdefinierte Anforderung	Modellierung durch Baustein(e) des IT-Grundschutz-Kompendiums	Anforderung in CON.2.bd.1 *Generische Maßnahmen im SDM*
D.1.4 Aufz. 1	Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten (B1.2 Zweckbindung)	Für Verarbeitungstätigkeit MÜSSEN Verarbeitungs-, Nutzungs- und Übermittlungsrechte auf das notwendige Minimum beschränkt werden.		CON.2.bd.1.A13 Beschränkung von Verarbeitungstätigkeiten (B) [Fachverantwortliche]
D.1.4 Aufz. 2	Programmtechnische Unterlassung bzw. Schließung von Schnittstellen bei Verarbeitungsverfahren und Komponenten (B1.2 Zweckbindung)	Für Verarbeitungstätigkeit DÜRFEN KEINE Schnittstellen aktiviert oder entwickelt werden, die nicht dem rechtmäßigen Zweck dienen.		CON.2.bd.1.A13 Beschränkung von Verarbeitungstätigkeiten (B) [Fachverantwortliche]
D.1.4 Aufz. 3	Regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung (B1.2 Zweckbindung)	Verarbeitungstätigkeiten DÜRFEN KEINE Backdoors enthalten. Das Verbot MUSS schriftlich dokumentiert werden. Die Einhaltung des Verbots im Rahmen der Softwareentwicklung MUSS sichergestellt werden.		CON.2.bd.1.A13 Beschränkung von Verarbeitungstätigkeiten (B) [Fachverantwortliche]
D.1.4 Aufz. 4	Trennung nach Organisations-/Abteilungsgrenzen (B1.2 Zweckbindung)		Der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

D.1.4 Aufz. 5	Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentifizierungsverfahrens (B1.2 Zweckbindung)		Der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* MUSS einmal auf den gesamten Informationsverbund angewendet werden. Bei der Modellierung einer Verarbeitungstätigkeit MÜSSEN neben den Basis-Anforderungen zusätzlich die folgenden Standard-Anforderungen angewendet werden: • ORP.4.A12 *Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen (S) [IT-Betrieb]* • ORP.4.A13 *Geeignete Auswahl von Authentisierungsmechanismen (S) [IT-Betrieb]* • ORP.4.A17 *Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen (S) [IT-Betrieb]*	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)] CON.2.bd.1.A2 Modellierung von Standard-Anforderungen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.4 Aufz. 6	Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle (B1.2 Zweckbindung)		Der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* MUSS einmal auf den gesamten Informationsverbund angewendet werden. Bei der Modellierung einer Verarbeitungstätigkeit MUSS neben den Basis-Anforderungen zusätzlich die folgende Standard-Anforderung angewendet werden: • ORP.4.A13 *Geeignete Auswahl von Authentisierungsmechanismen (S) [IT-Betrieb]*	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)] CON.2.bd.1.A2 Modellierung von Standard-Anforderungen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.4 Aufz. 7	Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten (B1.2 Zweckbindung)	Verarbeitungstätigkeiten MÜSSEN so gestaltet sein, dass möglichst Pseudonyme, Anonymisierungsdienste, anonyme Credentials und pseudonymisierte oder anonymisierte Daten verwendet werden.		CON.2.bd.1.A14 Pseudonymisierung und Anonymisierung von Daten (B) [Fachverantwortliche, IT-Betrieb]
D.1.4 Aufz. 8	Geregelte Zweckänderungsverfahren (B1.2 Zweckbindung)		Der Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* MUSS einmal auf den gesamten Informationsverbund angewendet werden. Bei der Modellierung einer Verarbeitungstätigkeit MÜSSEN neben den Basis-Anforderungen zusätzlich die folgenden Standard-Anforderungen angewendet werden: • OPS.1.1.3.A5 *Umgang mit Änderungsanforderungen (S) [Fachverantwortliche]*	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)] CON.2.bd.1.A2 Modellierung von Standard-Anforderungen (B) [Informationssicherheitsbeauftragte (ISB)]

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

			• OPS.1.1.3.A6 *Abstimmung von Änderungsanforderungen (S)* • OPS.1.1.3.A7 *Integration des Änderungsmanagements in die Geschäftsprozesse (S)*	

5.5 D.1.5 Transparenz

Typische Maßnahmen zur Gewährleistung der Transparenz gemäß SDM sind:

Nummer im SDM	Bezeichnung im SDM V.3.1	Modellierung durch eine neue benutzerdefinierte Anforderung	Modellierung durch Baustein(e) des IT-Grundschutz-Kompendiums	Anforderung in CON.2.bd.1 *Generische Maßnahmen im SDM*
D.1.5 Aufz. 1	Dokumentation im Sinne einer Inventarisierung aller Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO (B1.8 Rechenschafts- und Nachweisfähigkeit)	Es MUSS ein Verzeichnis der Verarbeitungstätigkeiten (VVT) gemäß Art. 30 DS-GVO angelegt werden.		CON.2.bd.1.A15 Zusätzliche Dokumentation bei Verarbeitungstätigkeiten (B) [Fachverantwortliche, IT-Betrieb]
D.1.5 Aufz. 2	Dokumentation der Bestandteile von Verarbeitungstätigkeiten insbesondere der Geschäftsprozesse, Datenbestände, Datenflüsse und Netzpläne, dafür genutzte IT-Systeme, Betriebsabläufe, Beschreibungen von Verarbeitungstätigkeiten, Zusammenspiel mit anderen Verarbeitungstätigkeiten (B1.8 Rechenschafts- und Nachweisfähigkeit)	Das Verzeichnis der Verarbeitungstätigkeiten (VVT) MUSS die folgenden Angaben enthalten: • Geschäftsprozesse • Datenbestände • Datenflüsse • Netzpläne • genutzte IT-Systeme • Betriebsabläufe • Beschreibungen von Verarbeitungstätigkeiten • Zusammenspiel mit anderen Verarbeitungstätigkeiten		CON.2.bd.1.A15 Zusätzliche Dokumentation bei Verarbeitungstätigkeiten (B) [Fachverantwortliche, IT-Betrieb]
D.1.5 Aufz. 3	Dokumentation von Tests, der Freigabe und ggf. der Datenschutz-Folgenabschätzung von neuen oder geänderten Verarbeitungstätigkeiten (B1.8 Rechenschafts- und Nachweisfähigkeit)	Falls die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, MUSS eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden.	Die Bausteine • OPS.1.1.6 *Software-Tests und -Freigaben* • OPS.1.1.3 *Patch- und Änderungsmanagement* MÜSSEN einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A15 Zusätzliche Dokumentation bei Verarbeitungstätigkeiten (B) [Fachverantwortliche, IT-Betrieb] CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.5 Aufz. 4	Dokumentation der Faktoren, die für eine Profilierung, zum Scoring oder für teilautomatisierte Entscheidungen genutzt werden (B1.8 Rechenschafts- und Nachweisfähigkeit)	Die folgenden Informationen MÜSSEN dokumentiert werden: • …		CON.2.bd.1.A15 Zusätzliche Dokumentation bei Verarbeitungstätigkeiten (B) [Fachverantwortliche, IT-Betrieb]

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

		• Faktoren, die für eine Profilierung, zum Scoring oder für teilautomatisierte Entscheidungen genutzt werden • …		
D.1.5 Aufz. 5	Dokumentation der Verträge mit den internen Mitarbeitenden, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen (B1.8 Rechenschafts- und Nachweisfähigkeit)	Die folgenden Informationen MÜSSEN dokumentiert werden: • … • Verträge mit Personen und Organisationen, von denen Daten erhoben bzw. an die Daten übermittelt werden • …	Die Bausteine • ORP.1 *Organisation* • ORP.2 *Personal* MÜSSEN einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A15 Zusätzliche Dokumentation bei Verarbeitungstätigkeiten (B) [Fachverantwortliche, IT-Betrieb] CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.5 Aufz. 6	Dokumentation von Einwilligungen, deren Widerruf sowie Widersprüche (B2 Einwilligungsmanagement)	Die folgenden Informationen MÜSSEN dokumentiert werden: • … • Einwilligungen zu einer Verarbeitung, deren Widerruf sowie Widersprüche	Der Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A15 Zusätzliche Dokumentation bei Verarbeitungstätigkeiten (B) [Fachverantwortliche, IT-Betrieb] CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.5 Aufz. 7	Protokollierung von Zugriffen und Änderungen (B1.23 Angemessene Überwachung der Verarbeitung, B1.8 Rechenschafts- und Nachweisfähigkeit)		Der Baustein OPS.1.1.5 *Protokollierung* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.5 Aufz. 8	Versionierung (B1.23 Angemessene Überwachung der Verarbeitung, B1.8 Rechenschafts- und Nachweisfähigkeit)	Verarbeitungstätigkeiten MÜSSEN so gestaltet sein, dass eine Versionierung und Änderungsverfolgung ermöglicht wird.		CON.2.bd.1.A16 Sicherstellung einer Versionierung und Änderungsverfolgung (B) [Fachverantwortliche, IT-Betrieb]
D.1.5 Aufz. 9	Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts (B1.23 Angemessene Überwachung der Verarbeitung, B1.8 Rechenschafts- und Nachweisfähigkeit)		Der Baustein OPS.1.1.5 *Protokollierung* MUSS einmal auf den gesamten Informationsverbund angewendet werden. Bei der Modellierung einer Verarbeitungstätigkeit MUSS neben den Basis-Anforderungen zusätzlich die folgende Standard-Anforderung angewendet werden: • OPS.1.1.5.A9 *Bereitstellung von Protokollierungsdaten für die Auswertung (S)* Bei der Modellierung einer Verarbeitungstätigkeit MÜSSEN neben den Basis-Anforderungen aller modellierten Bausteine jeweils die Standard-Anforderungen bzw. die Anforderungen für erhöhten Schutzbedarf angewendet werden, die eine Auswertung von Protokollen fordern. Dies sind insbesondere: • APP.3.6.A15 *Auswertung der Logdaten (S)*	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)] CON.2.bd.1.A2 Modellierung von Standard-Anforderungen (B) [Informationssicherheitsbeauftragte (ISB)] CON.2.bd.1.A3 Modellierung von Anforderungen für erhöhten Schutzbedarf (B) [Informationssicherheitsbeauftragte (ISB)]

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

			• DER.1.A6 *Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten (S)* • DER.1.A14 *Auswertung der Protokollierungsdaten durch spezialisiertes Personal (H)*	
D.1.5 Aufz. 10	Dokumentation der Quellen von Daten, bspw. des Umsetzens der Informationspflichten gegenüber Betroffenen, wo deren Daten erhoben wurden sowie des Umgangs mit Datenpannen (B1.1 Transparenz für Betroffene, B1.8 Rechenschafts- und Nachweisfähigkeit)	Die folgenden Informationen MÜSSEN dokumentiert werden: • Quelle von Daten • Art der Umsetzung der Informationspflichten gegenüber Betroffenen, • wo deren Daten erhoben wurden • Umgangs mit Datenpannen • …		CON.2.bd.1.A15 Zusätzliche Dokumentation bei Verarbeitungstätigkeiten (B) [Fachverantwortliche, IT-Betrieb]
D.1.5 Aufz. 11	Benachrichtigung von Betroffenen bei Datenpannen oder bei Weiterverarbeitungen zu einem anderen Zweck (B1.1 Transparenz für Betroffene)	Betroffene MÜSSEN bei Datenpannen oder bei Weiterverarbeitungen zu einem anderen Zweck benachrichtigt werden.		CON.2.bd.1.A17 Information und Benachrichtigung von Betroffenen (B) [Fachverantwortliche, Informationssicherheitsbeauftragte (ISB), Datenschutzbeauftragte]
D.1.5 Aufz. 12	Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte (B1.1 Transparenz für Betroffene)	Die Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte MÜSSEN nachverfolgbar sein.		CON.2.bd.1.A18 Nachverfolgung der Aktivitäten der verantwortlichen Stelle zur Gewährung von Betroffenenrechten (B) [Institutionsleitung, Fachverantwortliche]
D.1.5 Aufz. 13	Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept (B1.1 Transparenz für Betroffene)	Auskunftsrechte von Betroffenen MÜSSEN im Protokollierungs- und Auswertungskonzept berücksichtigt werden.		CON.2.bd.1.A19 Berücksichtigung von datenschutzrechtlichen Anforderungen im Protokollierungs- und Auswertungskonzept B) [Informationssicherheitsbeauftragte (ISB)]
D.1.5 Aufz. 14	Bereitstellung von Informationen über die Verarbeitung von personenbezogenen Daten an Betroffene (B1.1 Transparenz für Betroffene)	Betroffenen MÜSSEN Informationen über die Verarbeitung von personenbezogenen Daten bereitgestellt werden.		CON.2.bd.1.A17 Information und Benachrichtigung von Betroffenen (B) [Fachverantwortliche, Informationssicherheitsbeauftragte (ISB), Datenschutzbeauftragte]

5.6 D.1.6 Intervenierbarkeit

Typische Maßnahmen zur Gewährleistung der Intervenierbarkeit gemäß SDM sind:

Nummer im SDM	Bezeichnung im SDM V.3.1	Modellierung durch eine neue benutzerdefinierte Anforderung	Modellierung durch Baustein(e) des IT-Grundschutz-Kompendiums	Anforderung in CON.2.bd.1 *Generische Maßnahmen im SDM*
D.1.6 Aufz. 1	Maßnahmen für differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten (B2 Einwilligungsmanagement)	Verfahren zu einer differenzierten Einwilligung zu einer Verarbeitung, deren Widerruf sowie		CON.2.bd.1.A20 Etablieren von Verfahren zu Einwilligungen zu einer Verarbeitung, deren

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

		Verfahren für Widersprüche MÜSSEN vorhanden sein.		Widerruf sowie Widersprüchen (B) [Institutionsleitung, Fachverantwortliche]
D.1.6 Aufz. 2	Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen (B1.11 Berichtigungsmöglichkeit von Daten, B1.13 Einschränkbarkeit der Verarbeitung, B1.17 Datenschutz durch Voreinstellungen, B2 Einwilligungsmanagement, B3 Umsetzung aufsichtsbehördlicher Anordnungen)	Die Verarbeitungstätigkeit MUSS insbesondere die folgenden Datenfelder enthalten: • Sperrkennzeichen • Benachrichtigungen • Einwilligungen • Widersprüche • Gegendarstellungen		CON.2.bd.1.A21 Bereitstellung von Datenfeldern (B) [Fachverantwortliche, IT-Betrieb]
D.1.6 Aufz. 3	Dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen an Verarbeitungstätigkeiten sowie an den technischen und organisatorischen Maßnahmen (B1.22 Behebung und Abmilderung von Datenschutzverletzungen, B1.13 Einschränkbarkeit der Verarbeitung, B3 Umsetzung aufsichtsbehördlicher Anordnungen)		Der Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* MUSS einmal auf den gesamten Informationsverbund angewendet werden.	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.6 Aufz. 4	Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem (B1.22 Behebung und Abmilderung von Datenschutzverletzungen, B1.13 Einschränkbarkeit der Verarbeitung, B3 Umsetzung aufsichtsbehördlicher Anordnungen)	Die Verarbeitungstätigkeit MUSS eine Deaktivierungsmöglichkeit einzelner Funktionalitäten bieten, ohne das Gesamtsystem in Mitleidenschaft zu ziehen.		CON.2.bd.1.A22 Umsetzung einer datenschutzkonformen Systemarchitektur (B) [Institutionsleitung, Fachverantwortliche, IT-Betrieb]
D.1.6 Aufz. 5	Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten)	Die Verarbeitungstätigkeit MUSS standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen besitzen.		CON.2.bd.1.A22 Umsetzung einer datenschutzkonformen Systemarchitektur (B) [Institutionsleitung, Fachverantwortliche, IT-Betrieb]
D.1.6 Aufz. 6	Betreiben einer Schnittstelle für strukturierte, maschinenlesbare Daten zum Abruf durch Betroffene (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten, B1.14 Datenübertragbarkeit)	Die Verarbeitungstätigkeit MUSS eine Schnittstelle für strukturierte, maschinenlesbare Daten zum Abruf durch Betroffene besitzen.		CON.2.bd.1.A22 Umsetzung einer datenschutzkonformen Systemarchitektur (B) [Institutionsleitung, Fachverantwortliche, IT-Betrieb]
D.1.6 Aufz. 7	Identifizierung und Authentifizierung der Personen, die Betroffenenrechte wahrnehmen möchten (B1.9 Identifizierung und Authentifizierung)	Die Institution MUSS Personen, die Betroffenenrechte wahrnehmen möchten identifizieren und authentifizieren.		CON.2.bd.1.A23 Umsetzung von institutionellen Vorgaben (B) [Institutionsleitung, Fachverantwortliche]
D.1.6 Aufz. 8	Einrichtung eines Single Point of Contact (SPoC) für Betroffene (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten)	Die Institution MUSS einen Single Point of Contact (SPoC) für Betroffene einrichten.		CON.2.bd.1.A23 Umsetzung von institutionellen Vorgaben (B) [Institutionsleitung, Fachverantwortliche]
D.1.6 Aufz. 9	Operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten (B1.11	Die Institution MUSS operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung,		CON.2.bd.1.A22 Umsetzung einer datenschutzkonformen Systemarchitektur (B)

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

	Berichtigungsmöglichkeit von Daten, B1.12 Löschbarkeit von Daten, B1.13 Einschränkbarkeit der Verarbeitung von Daten, B1.14 Datenübertragbarkeit, B3 Umsetzung aufsichtsbehördlicher Anordnungen)	Sperrung und Löschung aller zu einer Person gespeicherten Daten bereitstellen.		[Institutionsleitung, Fachverantwortliche, IT-Betrieb]
D.1.6 Aufz. 10	Bereitstellen von Optionen für Betroffene, um Programme datenschutzgerecht einstellen zu können (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten, B1.17 Datenschutz durch Voreinstellungen)	Die Institution MUSS Optionen für Betroffene bereitstellen, um Programme datenschutzgerecht einstellen zu können.		CON.2.bd.1.A23 Umsetzung von institutionellen Vorgaben (B) [Institutionsleitung, Fachverantwortliche]

5.7 D.1.7 Datenminimierung

Das Gewährleistungsziel Datenminimierung kann gemäß SDM erreicht werden durch:

Nummer im SDM	Bezeichnung im SDM V.3.1	Modellierung durch eine neue benutzerdefinierte Anforderung	Modellierung durch Baustein(e) des IT-Grundschutz-Kompendiums	Anforderung in CON.2.bd.1 *Generische Maßnahmen im SDM*
D.1.7 Aufz. 1	Reduzierung von erfassten Attributen der betroffenen Personen (B1.3 Datenminimierung)	Die Verarbeitungstätigkeit DARF KEINE für den spezifischen Verarbeitungszweck unnötigen Attribute zu betroffenen Personen erfassen.		CON.2.bd.1.A24 Reduzierung datenschutzrelevanter Informationen und Vorgänge (B) [Institutionsleitung, Fachverantwortliche, IT-Betrieb]
D.1.7 Aufz. 2	Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten (B1.3 Datenminimierung)	Die Verarbeitungstätigkeit DARF KEINE für den spezifischen Verarbeitungszweck unnötigen Verarbeitungsoptionen in Verarbeitungsprozessschritten enthalten.		CON.2.bd.1.A24 Reduzierung datenschutzrelevanter Informationen und Vorgänge (B) [Institutionsleitung, Fachverantwortliche, IT-Betrieb]
D.1.7 Aufz. 3	Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten (B1.3 Datenminimierung)	Die Verarbeitungstätigkeit DARF KEINE für den spezifischen Verarbeitungszweck unnötigen Möglichkeiten der Kenntnisnahme vorhandener Daten bereitstellen.		CON.2.bd.1.A24 Reduzierung datenschutzrelevanter Informationen und Vorgänge (B) [Institutionsleitung, Fachverantwortliche, IT-Betrieb]
D.1.7 Aufz. 4	Festlegung von Voreinstellungen für betroffene Personen, die die Verarbeitung ihrer Daten auf das für den Verarbeitungszweck erforderliche Maß beschränken. (B1.17 Datenschutz durch Voreinstellungen)	Die Verarbeitungstätigkeit MUSS so voreingestellt sein, dass die Verarbeitung von Daten auf das für den spezifischen Verarbeitungszweck erforderliche Maß beschränkt ist.		CON.2.bd.1.A22 Umsetzung einer datenschutzkonformen Systemarchitektur (B) [Institutionsleitung, Fachverantwortliche, IT-Betrieb]
D.1.7 Aufz. 5	Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen (B1.3 Datenminimierung)	Die Verarbeitungstätigkeit SOLLTE so entwickelt und konfiguriert sein, dass automatisierte Verarbeitungsprozesse (nicht Entscheidungsprozesse), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen bevorzugt werden.		CON.2.bd.1.A22 Umsetzung einer datenschutzkonformen Systemarchitektur (B) [Institutionsleitung, Fachverantwortliche, IT-Betrieb]
D.1.7 Aufz. 6	Implementierung von Datenmasken, die Datenfelder unterdrücken, sowie automatischer Sperr- und Löschroutinen, Pseudonymisierungs-	Für die Verarbeitungstätigkeit MÜSSEN Datenfelder maskiert werden, falls ihre vollständige oder teilweise Anzeige für den spezifischen Verarbeitungszweck unnötig ist.		CON.2.bd.1.A22 Umsetzung einer datenschutzkonformen Systemarchitektur (B) [Institutionsleitung, Fachverantwortliche, IT-Betrieb]

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)

	und Anonymisierungsverfahren (B1.3 Datenminimierung, B1.5 Speicherbegrenzung)	Für die Verarbeitungstätigkeit MÜSSEN Datenfelder mit automatischen Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren ausgestattet werden, falls ihre dauerhafte Verarbeitung ohne diese Maßnahmen für den spezifischen Verarbeitungszweck unnötig ist.		
D.1.7 Aufz. 7	Festlegung und Umsetzung eines Löschkonzepts (B1.5 Speicherbegrenzung)		Der Baustein CON.6 *Löschen und Vernichten* MUSS einmal auf den gesamten Informationsverbund angewendet werden. Bei der Modellierung einer Verarbeitungstätigkeit MUSS neben den Basis-Anforderungen zusätzlich die folgende Standard-Anforderung angewendet werden: • CON.6.A8 Erstellung einer Richtlinie für die Löschung und Vernichtung von Informationen (S) [Mitarbeitende, IT-Betrieb, Datenschutzbeauftragte]	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)] CON.2.bd.1.A2 Modellierung von Standard-Anforderungen (B) [Informationssicherheitsbeauftragte (ISB)]
D.1.7 Aufz. 8	Regelungen zur Kontrolle von Prozessen zur Änderung von Verarbeitungstätigkeiten (B1.3 Datenminimierung)		Der Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* MUSS einmal auf den gesamten Informationsverbund angewendet werden. Bei der Modellierung einer Verarbeitungstätigkeit MÜSSEN neben den Basis-Anforderungen zusätzlich die folgenden Standard-Anforderungen angewendet werden: • OPS.1.1.3.A5 Umgang mit Änderungsanforderungen (S) [Fachverantwortliche] • OPS.1.1.3.A6 Abstimmung von Änderungsanforderungen (S) • OPS.1.1.3.A7 Integration des Änderungsmanagements in die Geschäftsprozesse (S)	CON.2.bd.1.A1 Modellierung von Bausteinen (B) [Informationssicherheitsbeauftragte (ISB)] CON.2.bd.1.A2 Modellierung von Standard-Anforderungen (B) [Informationssicherheitsbeauftragte (ISB)]

Herausgeber: CycleSEC GmbH, Hamburg | Versionsstand: 0.9.0 (ENTWURF)