DSB-5seenland.de

DS-Umsetzung im Unternehmen

Standarddatenschutzmodell vs. BSI-Grundschutz

DSB-5seenland.de

Titel	SDM 3.0	BSI-Grundschutz
Schutzobjekt	Rechte und Freiheiten natürlicher Personen	Alle Daten einer Organisation
Schutzziel	Gewährleistungsziele gem. SDM • Datenminimierung • **Verfügbarkeit** • **Integrität** • **Vertraulichkeit** • Nichtverkettung von Zwecken • Transparenz • Intervenierbarkeit	Schutzziele der Organisation • Authentizität • **Verfügbarkeit** • **Integrität** • **Vertraulichkeit** • Verbindlichkeit • Zuverlässigkeit • Resilienz/Belastbarkeit • Nichtabstreitbarkeit

Standarddatenschutzmodell vs. BSI-Grundschutz

DSB-5seenland.de

Titel	SDM 3.0	BSI-Grundschutz
Anwendungsbereich	Datenschutzrechtlich konforme Gestaltung der Verarbeitung personenbezogener Daten. Keine Anforderungen über das Datenschutzrecht hinaus	Beschreibung standardisierter Sicherheitsanforderungen für typische Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen, Gebäude und Räume. Ziel ist es, einen angemessenen Schutz für alle Informationen einer Institution zu erreichen.
Anwendungs-verpflichtung	Rechtliche Verpflichtung zur Umsetzung durch Datenschutzgesetze	Keine
Risikobewertung aus Schadenshöhe und Eintrittswahrscheinlichkeit	Keine mathematisch-statistische Bewertung möglich, da Rechte und Freiheiten geschützt werden. Daher Bildung individueller Risikokategorien notwendig.	Schadenshöhe kann mathematisch festgestellt werden, Eintrittswahrscheinlichkeit kann historisch-statistisch abgeleitet werden.

Grundsätze und Anforderungen/Gewährleistungsziele

DSB-5seenland.de

Datenminimierung

- Daten müssen dem Zweck angemessen, erheblich und auf das notwendige Maß beschränkt sein.
  - Angemessen – konkreter inhaltlicher Bezug zum Zweck
  - Erheblich – Beitrag zur Zweckerreichung nötig
  - Beschränkt – ohne die Verarbeitung der Daten kann der Zweck nicht erreicht werden und es gibt keine anderen Mittel der Zweckerreichung
- Kann ein dynamische Prozess sein, so dass Daten im Verlauf pseudonymisiert werden müssen
- Daraus ergibt sich die frühestmögliche Löschung der Daten
- Datenminimierung reicht vom Design der Informationstechnik durch den Hersteller bis zu ihrem Einsatz in den Kernprozessen der Verarbeitung wie auch in den unterstützenden Prozessen zum Beispiel bei der Wartung der verwendeten Systeme.

Verfügbarkeit

- Anforderung, dass der Zugriff auf personenbezogene Daten und ihre Verarbeitung unverzüglich möglich ist und sie ordnungsgemäß im vorgesehenen Prozess verwendet werden können.
- Maßnahmen, die sicherstellen, dass personenbezogene Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können
- Maßnahmen, die die Verfügbarkeit der personenbezogenen Daten und der Systeme und Dienste, die diese verarbeiten, garantieren

Grundsätze und Anforderungen aus Art.5 DSGVO

DSB-5seenland.de

Integrität

- Anforderung, dass die informationstechnischen Prozesse und Systeme die Spezifikationen kontinuierlich einhalten, die zur Ausübung ihrer zweckbestimmten Funktionen für sie festgelegt wurden
- Daten müssen unversehrt, vollständig, richtig und aktuell bleiben.
- Dies gilt auch dann, wenn die unterliegenden Systeme und Dienste unerwartet hoher Last unterliegen
- Neben dem Aspekt der Fehlerfreiheit muss gerade bei automatisierten Bewertungs- und Entscheidungsprozessen der Aspekt der Diskriminierungsfreiheit gewahrt werden
- Es sind Maßnahmen zur Bereinigung von Trainingsdaten und der Validierung von Ergebnissen bei der Anwendung von KI-Verfahren zu ergreifen

Vertraulichkeit

- Anforderung, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen oder nutzen kann
- Die Vertraulichkeit personenbezogener Daten ist auch dann sicherzustellen, wenn die unterliegenden Systeme und Dienste unerwartet hoher Last unterliegen

Grundsätze und Anforderungen aus Art.5 DSGVO

DSB-5seenland.de

Transparenz

- Verantwortliche Stelle muss geeignete Maßnahmen treffen, um der betroffenen alle Informationen in Bezug auf die Verarbeitungstätigkeit zu übermitteln
- Information hat unverzüglich, spätestens aber nach 1 Monat über dem Stand der Bearbeitung und die getroffenen Maßnahmen zu erfolgen
- Meldepflicht bei Datenpannen

Nichtverkettung

- PbD dürfen nicht zusammengeführt, also verkettet, werden. Insbesondere, wenn die Daten zu verschiedenen Zwecken erhoben wurden.
- Die Nichtverkettung soll durch technische und organisatorische Maßnahmen sichergestellt werden, z.B. Pseudonymisierung, Maßnahmen mit denen systemseitig die Weiterverarbeitung getrennt von der Ursprungsverarbeitung erfolgt.

Grundsätze und Anforderungen aus Art.5 DSGVO

DSB-5seenland.de

Transparenz

- Verantwortliche Stelle muss geeignete Maßnahmen treffen, um der betroffenen alle Informationen in Bezug auf die Verarbeitungstätigkeit zu übermitteln
- Information hat unverzüglich, spätestens aber nach 1 Monat über dem Stand der Bearbeitung und die getroffenen Maßnahmen zu erfolgen
- Meldepflicht bei Datenpannen

Intervenierbarkeit

- Betroffenen Personen müssen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und Erwirkung des Eingriffs in automatisierte Einzelentscheidungen bei Bestehen der gesetzlichen Voraussetzungen unverzüglich und wirksam gewährt werden können
- Soweit der Verantwortliche über Informationen verfügt, die es ihm erlauben, die betroffenen Personen zu identifizieren, muss er auch Maßnahmen zur Identifizierung und Authentifizierung der betroffenen Personen, die ihre Rechte wahrnehmen möchten, treffen
- Für informationstechnische Verarbeitungen, auf die betroffene Personen selbst Zugriff haben, müssen die Betroffenen in der Lage sein, Konfigurationen differenziert nach den jeweiligen Verarbeitungszwecken selbst vorzunehmen und zu entscheiden, welche Verarbeitungen sie gestatten wollen, die über das erforderliche Minimum hinausgehen.

Maßnahmen

Verfügbarkeit

Typische Maßnahmen zur Gewährleistung der Verfügbarkeit sind:

- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien,
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt)
- Behebung und Abmilderung von Datenschutzverletzungen),
- Dokumentation der Syntax der Daten
- Redundanz von Hard- und Software sowie Infrastruktur
- Umsetzung von Reparaturstrategien und Ausweichprozessen
- Erstellung eines Notfallkonzepts zur Wiederherstellung einer Verarbeitungstätigkeit
- Vertretungsregelungen für abwesende Mitarbeitende.

Maßnahmen

Integrität

- Einschränkung von Schreib- und Änderungsrechten
- Einsatz von Prüfsummen, elektronischen Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptokonzepts
- dokumentierte Zuweisung von Berechtigungen und Rollen
- Löschen oder Berichtigen falscher Daten
- Härten von IT-Systemen, so dass diese keine oder möglichst wenige Nebenfunktionalitäten aufweisen
- Prozesse zur Aufrechterhaltung der Aktualität von Daten
- Prozesse zur Identifizierung und Authentifizierung von Personen und Gerätschaften
- Festlegung des Sollverhaltens von Prozessen und regelmäßiger Durchführung von Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen
- Festlegung des Sollverhaltens von Abläufen bzw. Prozessen und regelmäßiger Durchführung von Tests
- Schutz vor äußeren Einflüssen (Spionage, Hacking)

Maßnahmen

Vertraulichkeit

- Festlegung eines Berechtigungs- und Rollenkonzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle
- Implementierung eines sicheren Authentifizierungsverfahrens
- 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
- Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle
- spezifizierte, für die Verarbeitungstätigkeit ausgestattete Umgebungen (Gebäude, Räume)
- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen usw.)
- Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept)
- Schutz vor äußeren Einflüssen (Spionage, Hacking)

Maßnahmen

Nichtverkettung

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten
- programmtechnische Unterlassung bzw. Schließung von Schnittstellen bei Verarbeitungsverfahren und Komponenten
- regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung
- Trennung nach Organisations-/Abteilungsgrenzen
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten und eines sicheren Authentifizierungsverfahrens
- Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle
- Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten
- geregelte Zweckänderungsverfahren

Maßnahmen

DSB-5seenland.de

Transparenz

- Dokumentation im Sinne einer Inventarisierung aller Verarbeitungstätigkeiten (VVT)
- Dokumentation der Bestandteile von Verarbeitungstätigkeiten insbesondere der Geschäftsprozesse, Datenbestände, Datenflüsse und Netzpläne, dafür genutzte IT-Systeme, Betriebsabläufe, Beschreibungen von Verarbeitungstätigkeiten
- Dokumentation von Tests, der Freigabe und ggf. der Datenschutz-Folgenabschätzung von neuen oder geänderten Verarbeitungstätigkeiten
- Dokumentation der Faktoren, die für eine Profilierung, zum Scoring oder für teilautomatisierte Entscheidungen genutzt werden
- Dokumentation der Verträge mit den internen Mitarbeitenden, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden
- Dokumentation von Einwilligungen, deren Widerruf sowie Widersprüche
- Protokollierung von Zugriffen und Änderungen

Maßnahmen

Transparenz (2)

- Versionierung
- Dokumentation der Verarbeitungsprozesse auf der Basis eines Protokollierungs- und Auswertungskonzepts
- Dokumentation der Quellen von Daten
- Umgang mit Datenpannen
- Benachrichtigung von Betroffenen bei Datenpannen oder bei Weiterverarbeitungen zu einem anderen Zweck
- Bereitstellung von Informationen über die Verarbeitung von personenbezogenen Daten an Betroffene

Maßnahmen

Intervenierbarkeit

- Maßnahmen für differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten
- Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen
- dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen an Verarbeitungstätigkeiten sowie an den technischen und organisatorischen Maßnahmen
- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem
- Betreiben einer Schnittstelle für strukturierte, maschinenlesbare Daten zum Abruf durch Betroffene
- Identifizierung und Authentifizierung der Personen, die Betroffenenrechte wahrnehmen möchten
- operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten
- Bereitstellen von Optionen für Betroffene, um Programme datenschutzgerecht einstellen zu können

Maßnahmen

- **Datenminimierung**
- Reduzierung von erfassten Attributen der betroffenen Personen
- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten
- Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten
- Festlegung von Voreinstellungen für betroffene Personen, die die Verarbeitung ihrer Daten auf das für den Verarbeitungszweck erforderliche Maß beschränken.
- Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen
- Implementierung von Datenmasken, die Datenfelder unterdrücken, sowie automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren
- Festlegung und Umsetzung eines Löschkonzepts

Bausteine

DSB-5seenland.de

Analog zum BSI-Grundschutzmodell wurden auch für das SDM Bausteine veröffentlicht, die die Umsetzung datenschutzrechtlicher Maßnahmen in der Praxis erleichtern sollen.
Bisher existieren zum DSM die Bausteine:

SDM-V2.0_B_43_Protokollieren_V1.0a
SDM-V2.0_B11_Aufbewahren_V1.0
SDM-V2.0_B42_Dokumentieren_V1.0a
SDM-V2.0_B50_Trennen_V1.0
SDM-V2.0_B60_Löschen_und_Vernichten_V1.0a
SDM-V2.0_B61_Berichtigen_V1.0
SDM-V2.0_B62_Einschränken_V1.0
SDM-V2.0b_B41_Planen_Spezifizieren_V1.0
SDM-V2.0b_B51_Zugriffe_regeln_V1.0

Die Bausteine können von der Webseite des bsi heruntergeladen werden und sind frei verwendbar.