D1 Generische Maßnahmen

Für jede der vom SDM zu betrachtenden Komponente (Daten, Systeme und Dienste sowie Prozesse) werden für jedes der Gewährleistungsziele Referenzmaßnahmen benannt und beschrieben. Für jede der Maßnahmen sind auch die Auswirkungen auf den Erreichungsgrad von anderen, von der Maßnahme nicht direkt betroffene Gewährleistungsziele zu betrachten. So können bestimmte Einzelmaßnahmen zur Erreichung mehrerer Gewährleistungszielen beitragen.

In diesem Abschnitt werden generische technische und organisatorische Maßnahmen - aufgeführt, die in der Datenschutzprüfpraxis vieler Datenschutzaufsichtsbehörden seit vielen Jahren erprobt sind. Die Zuordnung dieser Maßnahmen zu den Gewährleistungszielen des SDM soll zeigen, dass sich die Datenschutzanforderungen sinnvoll strukturieren lassen und in der Folge systematisch umsetzen lassen. Die konkreten Referenzmaßnahmen finden sich im Referenzmaßnahmen-Katalog (im Anhang) wieder.

Die Anforderung der DS-GVO an die Evaluierbarkeit (siehe Abschnitt B1.21) ist nicht in einem Gewährleistungsziel im SDM abzubilden, sondern in einem zyklischen Prozess (Datenschutzmanagement-Prozess, siehe das Kap. D4 Datenschutzmanagement mit SDM) umzusetzen. Es wird gefordert, dass die technisch-organisatorischen Maßnahmen nicht lediglich nur einmalig zu implementieren sind, sondern dass sie regelmäßig auf ihre Wirksamkeit zu überprüfen sind. In diesem regelmäßig zu wiederholenden Prozess ist beispielsweise zu prüfen, ob die Maßnahmen noch angemessen sind.

D1.1 Verfügbarkeit

Typische Maßnahmen zur Gewährleistung der Verfügbarkeit sind:

- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß eines getesteten Konzepts (B1.20 Wiederherstellbarkeit),
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt) (B1.18 Verfügbarkeit, B1.19 Belastbarkeit, B1.23 Behebung und Abmilderung von Datenschutzverletzungen),
- Dokumentation der Syntax der Daten (B1.18 Verfügbarkeit, B1.20 Wiederherstellbarkeit),
- Redundanz von Hard- und Software sowie Infrastruktur (B1.20 Verfügbarkeit, B1.19 Belastbarkeit),
- Umsetzung von Reparaturstrategien und Ausweichprozessen (B1.19 Belastbarkeit, B1.20 Wiederherstellbarkeit, B1.23 Behebung und Abmilderung von Datenschutzverletzungen),
- Erstellung eines Notfallkonzepts zur Wiederherstellung einer Verarbeitungstätigkeit (B1.19 Belastbarkeit, B1.20 Wiederherstellbarkeit),
- Vertretungsregelungen für abwesende Mitarbeitende (B1.18 Verfügbarkeit).

D1.2 Integrität

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

- Einschränkung von Schreib- und Änderungsrechten (B1.6 Integrität),

- Einsatz von Prüfsummen, elektronischen Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptokonzepts (B1.6 Integrität, B1.4 Richtigkeit, B1.22 Überwachung der Verarbeitung, B1.23 Behebung und Abmilderung von Datenschutzverletzungen),
- dokumentierte Zuweisung von Berechtigungen und Rollen (B1.6 Integrität),
- Löschen oder Berichtigen falscher Daten (B1.4 Richtigkeit),
- Härten von IT-Systemen, so dass diese keine oder möglichst wenige Nebenfunktionalitäten aufweisen (B1.6 Integrität, B1.19 Belastbarkeit),
- Prozesse zur Aufrechterhaltung der Aktualität von Daten (B1.4 Richtigkeit),
- Prozesse zur Identifizierung und Authentifizierung von Personen und Gerätschaften (B1.6 Integrität),
- Festlegung des Sollverhaltens von Prozessen und regelmäßiges Durchführen 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),
- Festlegung des Sollverhaltens von Abläufen bzw. Prozessen und regelmäßiges Durch- führen von Tests zur Feststellbarkeit bzw. Feststellung der Ist-Zustände von Prozessen (B1.6 Integrität, B1.16 Fehler- und Diskriminierungsfreiheit beim Profiling, B1.22 Überwachung der Verarbeitung, B1.19 Belastbarkeit),
- Schutz vor äußeren Einflüssen (Spionage, Hacking) (B1.6 Integrität, B1.19 Belastbarkeit, B1.23 Behebung und Abmilderung von Datenschutzverletzungen).

D1.3 Vertraulichkeit

Typische Maßnahmen zur Gewährleistung der Vertraulichkeit sind:

- Festlegung eines Rechte- und Rollen-Konzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle (B1.7 Vertraulichkeit),
- Implementierung eines sicheren Authentifizierungsverfahrens (B1.7 Vertraulichkeit),
- 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),
- Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle (B1.7 Vertraulichkeit, B1.23 Behebung und Abmilderung von Datenschutzverletzungen),
- spezifizierte, für die Verarbeitungstätigkeit ausgestattete Umgebungen (Gebäude, Räume) (B1.7 Vertraulichkeit),
- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen usw.) (B1.7 Vertraulichkeit, B1.23 Behebung und Abmilderung von Datenschutzverletzungen),
- Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept) (B1.7 Vertraulichkeit),
- Schutz vor äußeren Einflüssen (Spionage, Hacking) (B1.7 Vertraulichkeit, Belastbarkeit, B1.23 Behebung und Abmilderung von Datenschutzverletzungen).

D1.4 Nichtverkettung

Typische Maßnahmen zur Gewährleistung der Nichtverkettung sind:

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten (B1.2 Zweckbindung),
- programmtechnische Unterlassung bzw. Schließung von Schnittstellen bei Verarbeitungsverfahren und Komponenten (B1.2 Zweckbindung),
- regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung (B1.2 Zweckbindung),
- Trennung nach Organisations-/Abteilungsgrenzen (B1.2 Zweckbindung),
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentifizierungsverfahrens (B1.2 Zweckbindung),
- Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle (B1.2 Zweckbindung),
- Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten (B1.2 Zweckbindung),
- geregelte Zweckänderungsverfahren (B1.2 Zweckbindung).

D1.5 Transparenz

Typische Maßnahmen zur Gewährleistung der Transparenz sind:

- Dokumentation im Sinne einer Inventarisierung alle Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO (B1.8 Rechenschafts- und Nachweisfähigkeit),
- 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),
- Dokumentation von Tests, der Freigabe und ggf. der Datenschutz-Folgenabschätzung von neuen oder geänderten Verarbeitungstätigkeiten (B1.8 Rechenschafts- und Nachweisfähigkeit),
- Dokumentation der Faktoren, die für eine Profilierung, zum Scoring oder für teilautomatisierte Entscheidungen genutzt werden (B1.8 Rechenschafts- und Nachweisfähigkeit),
- 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),
- Dokumentation von Einwilligungen, deren Widerruf sowie Widersprüche (B2 Einwilligungsmanagement),
- Protokollierung von Zugriffen und Änderungen (B1.22 Überwachung der Verarbeitung, B1.8 Rechenschafts- und Nachweisfähigkeit),
- Versionierung (B1.22 Überwachung der Verarbeitung, B1.8 Rechenschafts- und Nachweisfähigkeit),
- Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts (B1.22 Überwachung der Verarbeitung, B1.8 Rechenschafts- und Nachweisfähigkeit),
- 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),
- Benachrichtigung von Betroffenen bei Datenpannen oder bei Weiterverarbeitungen zu einem anderen Zweck (B1.1 Transparenz für Betroffene),
- Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte (B1.1 Transparenz für Betroffene),
- Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und

Auswertungskonzept (B1.1 Transparenz für Betroffene),
- Bereitstellung von Informationen über die Verarbeitung von personenbezogenen Daten an Betroffene (B1.1 Transparenz für Betroffene).

D1.6 Intervenierbarkeit

Typische Maßnahmen zur Gewährleistung der Intervenierbarkeit sind:

- Maßnahmen für differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten (B2 Einwilligungsmanagement),
- 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),
- dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen an Verarbeitungstätigkeiten sowie an den technischen und organisatorischen Maßnahmen (B1.23 Behebung und Abmilderung von Datenschutzverletzungen, B1.13 Einschränkbarkeit der Verarbeitung, B3 Umsetzung aufsichtsbehördlicher Anordnungen),
- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem (B1.23 Behebung und Abmilderung von Datenschutzverletzungen, B1.13 Einschränkbarkeit der Verarbeitung, B3 Umsetzung aufsichtsbehördlicher Anordnungen),
- Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten),
- Betreiben einer Schnittstelle für strukturierte, maschinenlesbare Daten zum Abruf durch Betroffene (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten, B1.14 Datenübertragbarkeit),
- Identifizierung und Authentifizierung der Personen, die Betroffenenrechte wahrnehmen möchten (B1.9 Identifizierung und Authentifizierung),
- Einrichtung eines Single Point of Contact (SPoC) für Betroffene (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten),
- operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten (B1.11 Berichtigungsmöglichkeit von Daten, B1.12 Löschbarkeit von Daten, B1.13 Einschränkbarkeit der Verarbeitung von Daten, B1.14 Datenübertragbarkeit, B3 Umsetzung aufsichtsbehördlicher Anordnungen),
- Bereitstellen von Optionen für Betroffene, um Programme datenschutzgerecht einstellen zu können (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten, B1.17 Datenschutz durch Voreinstellung).

D1.7 Datenminimierung

Das Gewährleistungsziel Datenminimierung kann erreicht werden durch:

- Reduzierung von erfassten Attributen der betroffenen Personen (B1.3 Datenminimierung),
- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten (B1.3 Datenminimierung),
- Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten (B1.3 Datenminimierung),
- Festlegung von Voreinstellungen für betroffene Personen, die die Verarbeitung ihrer Daten auf

das für den Verarbeitungszweck erforderliche Maß beschränken. (B1.17 Datenschutz durch Voreinstellungen),
- 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),
- Implementierung von Datenmasken, die Datenfelder unterdrücken, sowie automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren (B1.3 Datenminimierung, B1.5 Speicherbegrenzung),
- Festlegung und Umsetzung eines Löschkonzepts (B1.5 Speicherbegrenzung),
- Regelungen zur Kontrolle von Prozessen zur Änderung von Verarbeitungstätigkeiten (B1.3 Datenminimierung).

D1.8 Gewährleistungsziele als Design-Strategie

Bereits bei der Modellierung von Verarbeitungstätigkeiten müssen für alle Ebenen die Anforderungen des Art. 25 DS-GVO berücksichtigt werden. Der dort formulierte Grundsatz der datenschutzfördernden Technikgestaltung („Data Protection by Design“) und datenschutzfreundlicher Voreinstellungen („Data Protection by Default“) verlangen eine Beachtung operativer Datenschutzanforderungen bereits während der Planungsphase einer Verarbeitung. Demnach sollen technische und organisatorische Maßnahmen nicht erst nachträglich festgelegt und umgesetzt werden, um ggf. nicht-rechtskonforme Funktionalitäten abzustellen. Datenschutzfreundliche Voreinstellungen verlangen auch, dass eine Fachapplikation von vornherein datenschutzkonform konfiguriert werden muss. Diese Grundsätze schließen das Prinzip der Datenminimierung als Design-Strategie ein.

Zur datenschutzgerechten Gestaltung der Funktionen der Verarbeitungstätigkeiten im Sinne von „Data Protection by Design“ können die Gewährleistungsziele des SDM als Design- Prinzip oder Design-Strategie interpretiert werden.

So verlangt das Gewährleitungsziel **Datenminimierung**, dass nicht mehr und nicht andere Daten erhoben werden als vom Zweck gedeckt sind. Datenschutzfreundliche Voreinstellungen sollen dazu führen, dass standardmäßig nur die personenbezogenen Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit (vgl. Art. 25 Abs. 2 DS-GVO). Die Gewährleistungsziele Datenminimierung und **Nichtverkettung** sind schon durch entsprechendes Design der für die Verarbeitung erforderlichen Informationstechnik umsetzbar. Beispielsweise muss der Funktionsumfang einer Fachapplikation allein auf die erforderlichen Funktionen reduziert werden. Zur Umsetzung des Gewährleistungsziels **Intervenierbarkeit** muss sichergestellt werden, dass die Betroffenenrechte tatsächlich von der Fachapplikation und aller weiteren IT-Dienste, die diese Applikation bspw. auf der Ebene der Infrastruktur nutzt, umsetzbar sind. Dies erfordert auch ausgereifte Changemanagement-Prozesse der Organisation. Diese Prozesse sind auch erforderlich, um auf Änderungen der rechtlichen Rahmenbedingungen reagieren zu können oder um neue, datenschutzfreundlichere Techniken in vorhandenen Verarbeitungen einsetzen zu können. Die Umsetzung des Gewährleitungsziels **Transparenz** bedeutet, dass von vornherein darauf geachtet wird, dass alle an Verarbeitungstätigkeiten direkt oder indirekt Beteiligten bzw. von diesen Betroffenen (Verantwortliche, Auftragsverarbeiter, die betroffenen Personen und Aufsichtsbehörden) entsprechend ihrer speziellen Interessen die Verarbeitungstätigkeiten prüfen können.