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.

D2 Verarbeitungstätigkeiten

Die DS-GVO verwendet „Verarbeitungstätigkeit“ in Art. 30 DS-GVO als zentralen Begriff des Datenschutzmanagements und definiert den Begriff der „Verarbeitung“ in Art. 4 Abs. 2 DS-GVO:

„Im Sinne dieser Verordnung bezeichnet der Ausdruck (...) Verarbeitung jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung; (...).“

Art. 30 DS-GVO listet die Angaben auf, die in das Verzeichnis der Verarbeitungstätigkeiten, das vom Verantwortlichen oder Auftragsverarbeiter zu führen ist, aufzunehmen sind. Genannt werden dort u. a.:

- Namen und Kontaktdaten des Verantwortlichen, des Vertreters sowie des Datenschutzbeauftragten,
- die Zwecke der Verarbeitung,
- eine Beschreibung der Kategorien betroffener Personen, personenbezogener Daten und Empfänger sowie ggfs. die Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation,
- die vorgesehenen Fristen für die Löschung,
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO.

Diese allgemeine Beschreibung einer Verarbeitung stellt noch keine ausreichende Dokumentation von Verarbeitungstätigkeiten dar und erfüllt allein noch nicht die Anforderungen an Transparenz gemäß Art. 5 Abs. 2 DS-GVO.

Die Funktion der vollständigen Dokumentation einer Verarbeitung besteht darin, dass alle relevanten Komponenten einer Verarbeitungstätigkeit aufgrund der bestehenden Rechenschaftspflicht prüffähig sind, um diese einer datenschutzrechtlichen Beurteilung unterziehen zu können. Prüffähigkeit bedeutet dabei, dass die Funktionen aller Komponenten, die bei einer Verarbeitungstätigkeit zum Einsatz kommen, insbesondere die Komponenten auf der Ebene der elektronischen Datenverarbeitung und Kommunikation, einer Soll-Ist-Bilanzierung zugänglich sind.

Diese Prüfbilanz bezüglich funktionaler Eigenschaften sowie der getroffenen technischen und organisatorischen Maßnahmen der Verarbeitungstätigkeit muss dann wiederum einer rechtlichen Beurteilung der Rechtskonformität bzw. Ordnungsmäßigkeit insgesamt unterzogen werden können unter der Fragestellung, ob die richtigen Maßnahmen zweckgemäß ausgewählt und mit der korrekten Wirkintensität betrieben werden.

D2.1 Ebenen einer Verarbeitung oder Verarbeitungstätigkeit

Um eine personenbezogene Verarbeitung vollständig zu erfassen, hat es sich bewährt, bei der Gestaltung oder Prüfung von Verarbeitungstätigkeiten zumindest drei verschiedene Ebenen der Darstellung wesentlicher Einflussgrößen oder Bestandteile zu unterscheiden. Wesentlich ist das Verständnis, dass eine „Verarbeitungstätigkeit“ bspw. nicht deckungsgleich mit der Verwendung einer bestimmten Technik oder eines bestimmten Fachprogramms ist.

Auf der **Ebene 1** ist eine personenbezogene Verarbeitung im datenschutzrechtlichen Sinne angesiedelt. Diese Verarbeitung findet bspw. im Rahmen eines privatrechtlich agierenden Unternehmens oder einer Behörde, die dem öffentlichen Recht unterliegt, statt, für deren Aktivitäten der Verantwortliche verantwortlich ist. Diese Ebene entspricht dem, was vielfach als ein „Fachverfahren“ und „Geschäftsprozess“ mit einem bestimmten funktionalen Ablauf der Verarbeitungstätigkeit verstanden wird. Auf dieser Ebene des Verständnisses einer Verarbeitung werden die für eine Verarbeitungstätigkeit erforderlichen personenbezogenen Daten sowie die gesetzlichen Anforderungen bestimmt. Der Verantwortliche definiert entsprechende Rollen und Berechtigungen an den personenbezogenen Daten und bestimmt die zu verwendenden IT-Systeme und Prozesse. Wesentlich für die datenschutzrechtlich angemessen funktionale Gestaltung dieser Ebene ist die **Bestimmung des Zwecks** oder der Zwecke der Verarbeitungstätigkeit.

Auf der **Ebene 2** ist die praktische Umsetzung der Verarbeitung und des Zwecks angesiedelt. Diese umfasst zum einen in der Regel die Rolle der Sachbearbeitung sowie die IT- Applikation(en), die sich genauer auch als „Fachapplikation eines Fachverfahrens“ bezeichnen lässt. Die Sachbearbeitung und die Fachapplikation müssen die funktionalen und (datenschutz-)rechtlichen Anforderungen, denen die Verarbeitung unterliegt, vollständig erfüllen. Die **Fachapplikation muss die Zweckbindung sicherstellen**. Die Applikation muss die Verarbeitung zusätzlicher Daten oder zusätzliche Verarbeitungsformen ausschließen, selbst wenn sie funktional besonders komfortabel sein mögen. Damit soll das Risiko minimiert werden, dass sie die Zweckbindung unterlaufen oder der Zweck überdehnt wird.

Auf der **Ebene 3** ist die IT-Infrastruktur angesiedelt, die Funktionen bereitstellt, die eine Fachapplikation der Ebene 2 nutzt. Zu dieser Ebene an „technischen Services“ zählen Betriebssysteme, virtuelle Systeme, Datenbanken, Authentifizierungs- und Autorisierungssysteme, Router und Firewalls, Speichersysteme wie SAN oder NAS, CPU- Cluster, sowie die Kommunikationsinfrastruktur einer Organisation wie das Telefon, das LAN, der Internetzugang oder der Betrieb von Webseiten. Auch hier gilt, dass diese Systeme innerhalb einer Verarbeitungstätigkeit jeweils so zu gestalten und zu nutzen sind, dass die **Zweckbindung erhalten** bleibt. Damit die Zweckbindung bzw. Zwecktrennung auf dieser Ebene durchgesetzt werden kann, müssen typischerweise technische und organisatorische Maßnahmen getroffen werden.

D2.2 Zweck

Ob eine Verarbeitung einem legitim gesetzten Zweck folgt und ob der Zweck der Verarbeitung hinreichend bestimmt ist, muss vor der Anwendung des SDM geklärt sein (siehe Abschnitt D4.2).

Bei der Umsetzung des spezifischen Zwecks einer Verarbeitung hat es sich bewährt, zwei weitere Aspekte zu beachten, um auch zu einer hinreichenden Zweckbindung der Verarbeitungstätigkeit zu gelangen:

- Zusätzlich zur Zweckbestimmung sind die Aspekte der **Zweckabgrenzung** bzw. der **Zwecktrennung** zu betrachten. So sollte festgelegt werden, welche (verwandte) Zwecke nicht mit der Verarbeitungstätigkeit umgesetzt werden sollen. Das erleichtert eine rechtskonforme Abtrennung der Verarbeitungstätigkeiten untereinander sowie insbesondere die Trennung von Datenbeständen, Systemen und Diensten sowie Prozessen auf der IT-Ebene.
- Es ist auch der Aspekt der **Zweckbindung** zu beachten. Die Zweckbindung einer Verarbeitung muss einerseits durch deren geeignete Funktionalität und durch geeignete Auswahl der zu verarbeitenden Produktions- oder Nutzdaten sichergestellt werden (horizontale Gestaltung). Die Zweckbindung einer Verarbeitung muss aber auch durch eine geeignete Ebenen-übergreifende

Gestaltung (siehe Abschnitt D2.1) sichergestellt werden (vertikale Gestaltung). So ist es in der Regel nicht vom Zweck abgedeckt und operativ auch nicht notwendig, dass neben den befugten Sachbearbeitern und deren Vorgesetzte auch noch IT-Administratoren, die beispielsweise auf der Ebene einer Datenbank die Zugriffsrechte verwalten, Kenntnis von den Inhalten der Verarbeitungsdaten nehmen können.

D2.3 Komponenten einer Verarbeitung oder Verarbeitungstätigkeit

Aus den Vorgaben der Datenschutz-Grundverordnung ergeben sich unmittelbar die Komponenten Daten, Systeme und Dienste. Bei der konkreten Modellierung von Verarbeitungstätigkeiten mit Personenbezug ist es jedoch notwendig, die folgenden drei Komponenten zu betrachten:

1. die personenbezogenen **Daten**,
2. die beteiligten technischen **Systeme und Dienste** (Hardware, Microservices, Software und Infrastruktur) ,
3. die technischen, organisatorischen und personellen **Prozesse** der Verarbeitung von Daten.

Der Ausdruck „Prozess“ ist in der DS-GVO nicht ausdrücklich enthalten. Jede Verarbeitungstätigkeit kann als Geschäftsprozess bzw. Fachverfahren modelliert werden; jede Verarbeitungstätigkeit besteht aus einzelnen Verarbeitungsschritten. Einzelne Verarbeitungen sind bspw. das Erheben, Erfassen, Ordnen oder Speichern bis zum Löschen oder Vernichten (vgl. Art. 4 Nr. 2 DS-GVO). Diese Verarbeitungen werden als Teilprozesse modelliert bzw. implementiert.

Methodisch stehen zunächst die Daten von Personen im Vordergrund, deren Erforderlichkeit der Verarbeitung an der Zweckbestimmung vorab zu bemessen ist.

Die konkrete funktionale Gestaltung geschieht auf der Ebene 1, auf der anhand der Daten der Schutzbedarf durch die verantwortliche Stelle festzustellen bzw. festzusetzen ist. Diesen Schutzbedarf erben alle Daten, Systeme und Prozesse, die bei einer konkreten Verarbeitung auf den verschiedenen Ebenen zum Einsatz kommen. Anhand des Referenzmaßnahmen- Katalogs kann überprüft werden, ob getroffene oder geplante technische und organisatorische Maßnahmen dem Schutzbedarf angemessen sind.

Bei diesen drei Kernkomponenten Daten, Systeme und Dienste sowie Prozesse spielen u. a. folgende spezielle Eigenschaften noch eine weitere zu beachtende Rolle:

Bei Daten sind Eigenschaften von **Datenformaten** zu betrachten, mit denen Daten erhoben und verarbeitet werden. Datenformate können Einfluss auf die Qualität der Umsetzung der Gewährleistungsziele haben, z. B. in den Fällen, in denen nicht als abschließend geklärt gelten darf, welche Inhalte Dateien mit bestimmten Formaten aufweisen. So können im Datenbestand von Textdateien vermeintlich gelöschte Daten enthalten sein, die im Ausdruck nicht erscheinen; Grafikdateien können Metadaten bspw. bzgl. Kameramodell, Ort und Zeit der Aufnahme enthalten oder es können wiederum relevante Informationen bei Grafik-, Video- und Audiodateien der Kompressionen zum Opfer fallen.

Bei den beteiligten Systemen sind die **Schnittstellen** zu betrachten, die eine Fachapplikation mit der Nutzung von IT-Systemen der Ebene 3 sowie insbesondere zu anderen Systemen, die nicht innerhalb der vom Zweck definierten Systemgrenze liegen, aufweist. Neben diesen vertikalen Schnittstellen sind auch horizontale Schnittstellen zu betrachten, mit denen ein Risiko für die Zweckbindung einhergeht. Der Ausweis der Existenz von Schnittstellen sowie die Dokumentation von deren Eigenschaften sind von entscheidender Bedeutung für die rechtliche Verantwortlichkeit,

Beherrschbarkeit und Prüfbarkeit von Datenflüssen.

Für jede Verarbeitungstätigkeit und deren Komponenten, insbesondere für die manchmal schwierig fassbaren Prozesse über verschiedene Systeme hinweg gilt, die **Verantwortlichkeit** zu verdeutlichen und im Verzeichnis der Verarbeitungstätigkeiten in Art. 30 DS-GVO zu dokumentieren. Gemäß Art. 4 Abs. 7 ist ein Verantwortlicher „(…) eine natürliche oder juristische Person, Behörde oder Einrichtung (…), die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet; (…).“ Aufgaben, die aus der Verantwortlichkeit resultieren, können in Form von individuellen Zuständigkeiten delegiert werden. Diese Zuständigkeiten werden typischerweise als Rollen in einem umfassenden Rollen- und Berechtigungskonzept formuliert und zugewiesen. Die Zuständigkeit eines Prozesseigentümers kann sich auf einzelne Verarbeitungen (Teilprozesse) oder auf die gesamte Verarbeitungstätigkeit über alle Prozessebenen hinweg im Sinne einer Gesamtzuständigkeit erstrecken. Diese Zuständigkeit kann auf unterschiedliche Rollen mit jeweils Teilzuständigkeiten verteilt werden. Wenn die Verarbeitungstätigkeit eine Auftragserarbeitung gemäß Art. 28 DS-GVO beinhaltet ist zu gewährleisten, dass der Auftragsverarbeiter seine Aufgaben gemäß den Weisungen des Verantwortlichen datenschutzkonform erfüllt.

Die Verantwortung für eine Verarbeitung liegt letztlich immer beim Verantwortlichen i. S. d. Art. 4 Abs. 7 DS-GVO.

D3 Risiken und Schutzbedarf

Die DS-GVO knüpft die Anforderungen an technische und organisatorische Maßnahmen an das mit der Verarbeitung der personenbezogenen Daten verbundene Risiko für die Rechte und Freiheiten betroffener Personen.

Im Kurzpapier Nr. 18 „Risiken für die Rechte und Freiheiten natürlicher Personen“ [1)] der Datenschutzkonferenz wird der Begriff des Risikos im Kontext der DS-GVO erläutert und in allgemeiner Form aufgezeigt, wie Risiken für die Rechte und Freiheiten natürlicher Personen bestimmt und in Bezug auf ihre Rechtsfolgen bewertet werden können. Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das einen Schaden für die Rechte und Freiheiten natürlicher Personen (einschließlich ungerechtfertigter Beeinträchtigung der Rechte und Freiheiten) darstellt oder zu einem Schaden für eine oder mehrere natürliche Personen führen kann. Es hat zwei Dimensionen: Erstens die Schwere des Schadens für die Rechte und Freiheiten der betroffenen Personen und zweitens die Wahrscheinlichkeit, dass das Ereignis und der Schaden eintreten. Gemäß ErwGr 75 sind unter die möglichen Schäden für die Rechte und Freiheiten natürlicher Personen physische, materielle und immaterielle Schäden einzuordnen. Im Folgenden wird allgemein von Schadensereignissen gesprochen. Ein Schadensereignis kann verschiedene Rechte und Freiheiten schädigen oder beeinträchtigen und möglicherweise weitere Schadensereignisse nach sich ziehen. Unrechtmäßige Verarbeitungstätigkeiten, insbesondere solche die nicht den Grundsätzen des Art. 5 DS-GVO entsprechen, sind in sich Beeinträchtigungen des Grundrechts auf Datenschutz und stellen daher bereits ein Schadensereignis dar. Sie können zusätzliche Schäden wie bspw. die Diskriminierung natürlicher Personen nach sich ziehen. [2)]

Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden.

Aufgabe des Verantwortlichen ist, diese Risiken zu identifizieren, zu analysieren und einzustufen und Maßnahmen zu deren Eindämmung zu treffen (siehe Kapitel D4 Datenschutzmanagement mit dem

SDM).

Dieses Kapitel D3 gibt Hilfestellungen, um das Datenschutz-Risiko einer Verarbeitungstätigkeit zu bestimmen. Es stellt außerdem den Zusammenhang her zwischen den Risiken durch eine Verarbeitungstätigkeit und dem durch sie hervorgerufenen Schutzbedarf natürlicher Personen bei der Verarbeitung personenbezogener Daten (Art. 1 Abs. 1 DS-GVO) einerseits und dem durch die implementierten Maßnahmen erreichten Schutzniveau bzw. dem Restrisiko einer Verarbeitungstätigkeit andererseits, mit dem Ziel, die Bestimmung geeigneter und angemessener Maßnahmen zu ermöglichen. Die Bestimmung der Höhe des Risikos ist die Voraussetzung dafür, technische und organisatorische Maßnahmen und den notwendigen Grad ihrer Wirksamkeit festlegen zu können, mit denen sich Risiken eliminieren oder zumindest reduzieren lassen und eine Verarbeitung datenschutzkonform erfolgen kann. Grundsätzlich gilt die Regel: Je höher das Risiko, desto umsichtiger muss die Verarbeitungstätigkeit gestaltet sein und desto wirksamer müssen die entsprechenden, konkreten technischen und organisatorische Maßnahmen betrieben, kontrolliert und ggf. verbessert werden.

D3.1 Risiken für Betroffene

a) Ausgangspunkt von Überlegungen zum Risiko ist die Verarbeitungstätigkeit, die aus einem oder mehreren Verarbeitungsvorgängen besteht. Es wird der in Art. 30 DS-GVO eingeführte Begriff „Verarbeitungstätigkeit“ verwendet, denn nach der Definition in Art. 4 Nr. 2 DS-GVO sind Verarbeitungen einzelne Vorgänge oder Vorgangsreihen. Für jede Verarbeitungstätigkeit müssen die in Art. 5 DS-GVO formulierten Grundsätze der Verarbeitung personenbezogener Daten beachtet werden. Das SDM „verdichtet“ diese Grundsätze zu Gewährleistungszielen, die weitere operative Anforderungen der DS-GVO aufnehmen. Jede Verarbeitungstätigkeit erzeugt grundsätzlich Risiken für betroffene Personen durch den Umstand der Verarbeitung personenbezogener Daten allein. Im Unterschied zum allgemeinen Risikomanagement und auch zum Risikomanagement in der Informationssicherheit besteht dabei im Bereich des Datenschutzes grundsätzlich die Pflicht, die durch die Verarbeitung personenbezogener Daten entstehenden Risiken mit geeigneten und angemessenen technischen und organisatorischen Maßnahmen auf ein angemessenes Schutzniveau zu reduzieren. Nach der DS-GVO ist es nicht zulässig, auf die Behandlung von Anforderungen insbesondere der Umsetzung der Grundsätze aus Art. 5 DS-GVO gänzlich zu verzichten und die daraus resultierenden Risiken in Kauf zu nehmen. Die aus dem Bereich der Informationssicherheit bekannten Instrumente der Risikoakzeptanz oder des Risikotransfers stehen im datenschutzrechtlichen Kontext dem Verantwortlichen nicht zur Verfügung. Spielraum besteht bei der Auswahl und der Art und Weise der Umsetzung von Anforderungen mit Hilfe von technischen und organisatorischen Maßnahmen, die in einen angemessenen Umfang gefordert werden (Artikel 5 Nr. 1 lit. d „angemessene Maßnahmen“, lit. f „angemessene Sicherheit“). Hier ist es geboten, bestehende Risiken für die Rechte und Freiheiten natürlicher Personen genauer zu analysieren. Erst wenn ein angemessenes Schutzniveau erreicht wurde und somit die Interessen der Betroffenen angemessen berücksichtigt wurden, können die verbleibenden Restrisiken durch den Verantwortlichen akzeptiert werden.

b) Art. 35 DS-GVO verlangt vom Verantwortlichen, bei einem „voraussichtlich hohen Risiko“ für die Rechte und Freiheiten natürlicher Personen eine Datenschutz- Folgenabschätzung für die vorgesehene Verarbeitung durchzuführen. Zur Bestimmung der Höhe des Risikos muss der Verantwortliche daher zunächst eine „Schwellwert- Analyse“ durchführen. Diese Analyse muss für jede Verarbeitungstätigkeit, bestehend aus einem oder mehreren Verarbeitungsvorgängen, durchgeführt werden, um die Entscheidung für die Einstufung einer Verarbeitungstätigkeit gegenüber einer zuständigen Datenschutzaufsichtsbehörde begründen zu können (Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO).

Wenn das Ergebnis der Schwellwert-Analyse ein „voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ ist, dann muss das eine Auswirkung auf die Gestaltung der Verarbeitungstätigkeit sowie deren Prüfbarkeit haben. Die methodisch zentrale Frage zur Gestaltung einer Verarbeitungstätigkeit besteht deshalb darin, wie für eine Verarbeitungstätigkeit die Höhe des Risikos zu bestimmen ist.

D3.2 Risikobetrachtung

D3.2.1 Schwellwert-Analyse

Ziel der Schwellwert-Analyse ist es festzustellen, ob eine Verarbeitungstätigkeit voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat und somit eine DSFA erfordert. Zur Identifikation eines voraussichtlich „hohen Risikos“ durch eine Verarbeitungstätigkeit wird folgendes Vorgehen vorgeschlagen, wobei die Reihenfolge nicht zwingend eingehalten werden muss:

1. Prüfen, ob die Verarbeitungstätigkeit, für welche das Risiko zu bestimmen ist, in der „Muss-Liste“ gemäß Art. 35 Abs. 4 DS-GVO der Datenschutzaufsichtsbehörden enthalten ist. Wenn ja, dann besteht ein voraussichtlich hohes Risiko. (Für den nicht-öffentlichen Bereich: https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf, Stand: 17.10.2018, letzter Aufruf: 01.04.2019).

2. Prüfen, ob die betrachtete Verarbeitungstätigkeit zu den besonders riskanten Verarbeitungstätigkeiten gem. Art. 35 Abs. 3 DS-GVO zählt. Wenn dies zutrifft, besteht ein voraussichtlich hohes Risiko.

3. Prüfen, ob auf die Verarbeitungstätigkeit Eigenschaften zutreffen, die in der Auflistung von Verarbeitungstätigkeiten mit „voraussichtlich hohem Risiko“ des Working Paper 248 rev. 01 [3)] des Europäischen Datenschutzausschusses enthalten sind. Wenn mindestens zwei der Einträge zutreffen ist in den meisten Fällen davon auszugehen, dass ein voraussichtlich hohes Risiko besteht. Ein hohes Risiko kann allerdings auch bereits dann vorliegen, wenn nur eines der Kriterien erfüllt ist.

1. Bewerten oder Einstufen (Scoring)
   („Evaluation or scoring“)
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
   („Automated-decicion making with legal or similar significant effect“)
3. Systematische Überwachung
   („Systematic monitoring“)
4. Vertrauliche Daten oder höchst persönliche Daten
   („Sensitive data or data of a highly personal nature“)
5. Datenverarbeitung in großem Umfang
   („Data processed in a large scale“)
6. Abgleichen oder Zusammenführen von Datensätzen
   („Matching or combining datasets“)
7. Daten zu schutzbedürftigen Betroffenen
   (Data concerning vulnerable data subjects“)
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
   („Innovative use or applying new technological or organisational solutions“)
9. Betroffene werden an der Ausübung ihres Rechts oder der Nutzung einer Dienstleistung bzw.

Durchführung eines Vertrages gehindert
(„When the processing in itself prevents data subjects from exercising a right or using a service or a contract“)

4. Prüfen, ob Art, Umfang, Umstände oder Zwecke (ErwG 76 DS-GVO) der Verarbeitungstätigkeit das Risiko für betroffene Personen erhöhen. Hierfür ist es ratsam, entsprechende Praxiserfahrungen und konkretisierende Gerichtsurteile in die Prüfung eines eventuell bestehenden hohen Risikos einzubeziehen.

D3.2.2 Risiko-Identifikation

Zur Identifikation konkreter Risiken für die Rechte und Freiheiten der betroffenen Personen, die auch durch spezifische Besonderheiten der Verarbeitungstätigkeit entstehen können, bietet es sich an, die folgenden Fragen zu stellen:

a) Welche Schäden können für betroffene Personen auf der Grundlage der zu verarbeitenden Daten auftreten?
b) Wodurch, d. h. durch welche Ereignisse kann es zu dem Schaden kommen?
c) Durch welche Handlungen und Umstände kann es zum Eintritt dieser Ereignisse kommen?

Insbesondere bei diesem Schritt kann es vorkommen, dass in Ausnahmefällen Risiken identifiziert werden, die zu sehr schwerwiegenden Auswirkungen für betroffene Personen führen können, etwa zu einer Gefahr für Leib und Leben. In solchen Fällen ist es sinnvoll, einen sehr hohen Schutzbedarf anzunehmen. Die durch das SDM vorgeschlagenen technischen und organisatorischen Maßnahmen sind dafür jedoch nicht ausgelegt, so dass in einem solchen Fall, wie auch bereits bei hohem Schutzbedarf, stets eine individuelle Betrachtung der möglichen Maßnahmen erfolgen muss, um ein entsprechendes angemessenes Schutzniveau herzustellen. Die Maßnahmen des SDM können jedoch als Ausgangspunkt für diese allgemeine Betrachtung dienen.

Neben den spezifischen Datenschutz-Risiken einer Verarbeitungstätigkeit selbst sind auch die Risiken der Informationssicherheit zu betrachten. Diese Risiken beziehen sich auf den Schutz der Geschäftsprozesse der Organisation. Zur Bearbeitung dieser Risiken hat sich der IT-Grundschutz des BSI bewährt (https://www.bsi.de). Wesentliche Aspekte von Grundschutz-Maßnahmen betreffen einen geordneten Betrieb, die Sicherstellung der Verfügbarkeit und Integrität der Daten, Systeme und Dienste sowie die Verhinderung eines unbefugten Zugriffs auf Geschäfts-, Produktions- und Personendaten, also die Sicherstellung der Vertraulichkeit. Diese sind Voraussetzungen auch für einen wirksamen Datenschutz. Sehr wichtig ist es, dabei darauf zu achten, dass bei der Abstimmung von Maßnahmen für die Informationssicherheit und den operativen Datenschutz insbesondere jene Schutzmaßnahmen, welche für die IT-Sicherheit betrieben werden, ihrerseits datenschutzkonform eingerichtet sind (z. B. Videoüberwachung zur Objektsicherung, Cloud- Lösungen zum Malwareschutz oder Protokollierung). Hierbei müssen etwaige Konflikte zwischen den Anforderungen des Datenschutzes und der Informationssicherheit aufgelöst werden.

D3.2.3 Risikobewertung

Es ist die Aufgabe des Verantwortlichen und ggfs. des Auftragsverarbeiters, die identifizierten Risiken für die betroffenen Personen zu analysieren und einzustufen. Dabei muss der Verantwortliche bzw. der Auftragsverarbeiter die Schwere und die Eintrittswahrscheinlichkeit der identifizierten Risiken nach objektiven Maßstäben bestimmen und dokumentieren. Aus dieser Bewertung folgt auf Basis

einer Risikofunktion (bspw. in Form einer Risikomatrix) die jeweilige Höhe der Risiken (vgl. Kurzpapier Nr. 18 „Risiken für die Rechte und Freiheiten natürlicher Personen“ [4)]).

D3.3 Risikohöhe, Schutzbedarfsstufe, Schutzniveau und Restrisiko

Der Schutzbedarf einer natürlichen Person bei der Verarbeitung personenbezogener Daten in Bezug auf ihre Rechte und Freiheiten ergibt sich aus dem Risiko, das von der Verarbeitungstätigkeit und deren Eingriffsintensität ausgeht. Die DS-GVO kennt nur die Begriffe „Risiko“ und „hohes Risiko“, wobei „Risiko“ hier als „normales Risiko“ bezeichnet wird. Daneben verwendet die DS-GVO die Formulierung „voraussichtlich nicht zu einem Risiko“ führend (Art. 27 Abs. 2 lit. a und Art. 33 Abs. 1 DS-GVO). Da es vollständig risikolose Verarbeitungen nicht geben kann, wird die Formulierung „nicht zu einem Risiko“ von ihrem Sinn und Zweck ausgehend als „nur zu einem geringen Risiko“ führend verstanden. Erfahrungen aus der Praxis zeigen, dass es solche geringen Risiken gibt, die in der DS-GVO keine gesonderte Erwähnung finden, für die jedoch ebenfalls Maßnahmen zu ergreifen sind. Die Maßnahmen für den normalen Schutzbedarf decken auch solche geringen Risiken ab.

Der Schutzbedarf ergibt sich aus dem Risiko der Verarbeitungstätigkeit, bevor technische und organisatorische Maßnahmen bestimmt und umgesetzt wurden. Insofern gilt der folgende Zusammenhang zwischen Risiko(höhe), im Sinne eines Ausgangsrisikos, und Schutzbedarf(sstufe):

- **kein oder geringes Risiko** der Verarbeitung → **normaler Schutzbedarf** für von der Verarbeitung betroffene Personen
- **normales Risiko** der Verarbeitung → **normaler Schutzbedarf** für von der Verarbeitung betroffene Personen
- **hohes Risiko** der Verarbeitung → **hoher Schutzbedarf** für von der Verarbeitung betroffene Personen

Während der durch das Ausgangsrisiko definierte Schutzbedarf betroffener Personen bzgl. der Verarbeitungstätigkeit konstant bleibt, können die Risiken der Verarbeitung für die betroffenen Personen durch technische und organisatorische Maßnahmen verringert werden. Diese Maßnahmen verändern nicht den Schutzbedarf, sondern reduzieren das Risiko der Verarbeitungstätigkeit. Die zunächst vorhandenen Risiken – die Ausgangsrisiken – müssen durch Verfahrensgestaltung und technische und organisatorische Maßnahmen so weit verringert werden, bis ein dem Risiko angemessenes (Art. 32 Abs. 1 DS-GVO) und somit verantwortbares Schutzniveau für die Verarbeitungstätigkeit gewährleistet wird. Oder anders ausgedrückt: Das Schutzniveau muss so hoch sein, dass die verbleibenden Restrisiken einer Verarbeitung durch den Verantwortlichen nachweislich berechtigt verantwortet werden können. Wenn kein angemessenes Restrisiko vorliegt, darf die Verarbeitungstätigkeit aufgrund mangelnder Rechtskonformität nicht aufgenommen werden. Verbleibt ein „hohes Risiko“ und darüber hinaus, dann sieht Art. 36 DS-GVO vor, dass der Verantwortliche die zuständige Datenschutzaufsichtsbehörde konsultieren muss.

Die Methodik des IT-Grundschutz des BSI nutzt zur Gewährleistung der Informationssicherheit ebenfalls das Konzept der Schutzbedarfseinstufungen, um die Wirkungen technischer und organisatorischer Maßnahmen skalieren zu können.

Wegen der unterschiedlichen Zielrichtungen von IT-Grundschutz des BSI (Gewährleistung der Informationssicherheit einer Organisation) und „operativem Datenschutz“ mit Hilfe des SDM (Gewährleistung der Rechte und Freiheiten natürlicher Personen) kann nicht ausgeschlossen werden, dass die Schutzbedarfsfeststellungen nach Grundschutz und nach SDM für dieselbe Verarbeitung unterschiedlich ausfallen. Kommt es zu unterschiedlichen Bewertungen, dann sollten entweder die

jeweiligen Maßnahmen für den höheren Schutzbedarf umgesetzt werden, oder es sollte im Rahmen einer genaueren Analyse festgestellt werden, was der Grund für die unterschiedlichen Bewertungen ist und wie in diesem Fall ein angemessenes Schutzniveau erzielt werden kann. Die datenschutzrechtlichen Anforderungen sind maßgeblich. Diese Analyse- und Entscheidungsprozesse mit ihrer dazugehörigen Bewertung sind zu dokumentieren. Sowohl bei einer unternehmens- oder organisationsinternen Evaluation bzw. Revision oder während einer datenschutzrechtlichen Prüfung mussnachvollziehbar sein, welche konkreten technischen und organisatorischen Maßnahmen zur Erlangung des erforderlichen Schutzniveaus in Bezug auf die jeweilige Verarbeitungstätigkeit ergriffen wurden.

D3.4 Bestimmung technischer und organisatorischer Maßnahmen insbesondere bei hohem Risiko

Grundsätzlich sind Datenverarbeitungsprozesse und damit die Spezifikation der Datenverarbeitung so zu gestalten, dass, wenn möglich, die Verarbeitung ohne Personenbezug erfolgt oder zumindest die Risiken gemindert werden. Wurde beispielsweise als Risiko identifiziert, dass in automatisierten Abrufverfahren hohe Risiken für die Rechte und Freiheiten natürlicher Personen bestehen, weil nicht erforderliche Abrufe nicht technisch unterbunden werden können oder der Datenumfang von Abrufen nicht vom Abrufenden angemessen eingeschränkt werden kann, so besteht eine weitere Möglichkeit zur Risikobeschränkung im Verzicht auf das automatisierte Abrufverfahren und eine ersatzweise Implementierung einer Übermittlung im Einzelfall. Beim Treffen geeigneter technischer und organisatorischer Maßnahmen ist der Stand der Technik zu berücksichtigen. Die in Abschnitt “D1 Generische Maßnahmen“ vorgeschlagenen technischen und organisatorischen Maßnahmen sind eine gute Grundlage, um angemessene Maßnahmen für normalen Schutzbedarf zu entwickeln. Zukünftig werden diese generischen Maßnahmen um den Referenzmaßnahmen-Katalog ergänzt. Im Fall eines hohen oder sehr hohen Schutzbedarfs wird die folgende standardisierte Strategie zur wirksamen Minderung der Risiken empfohlen.

1. Es sind die Maßnahmen des Referenzmaßnahmen-Katalogs umzusetzen, die bei normalem Ausgangsrisiko bzw. normalem Schutzbedarf zu ergreifen sind.
2. Zusätzliche Maßnahmen aus dem Referenzmaßnahmen-Katalog sind umzusetzen.
3. Zusätzlich sind individuelle Maßnahmen auszuwählen. Ein Beispiel für eine individuelle Maßnahme könnte darin bestehen, bestimmte Vorgänge einer Verarbeitungstätigkeit nur auf Antrag bzw. nach einer Prüfung freizugeben und diese Tätigkeit dann im Betrieb zu überwachen, so dass bei Abweichungen ein Abbruch oder die Korrekturmaßnahme ausgelöst wird.
4. Die Wirkung einer Maßnahme kann erhöht wird, indem Skalierungsmöglichkeiten genutzt werden.
   Ein Beispiel hierfür ist die Erhöhung der Länge eingesetzter kryptografischer Schlüssel. Ein anderes Beispiel wäre die Sicherung von Protokolldaten, der Betrieb dedizierter Protokolleserver für die Verarbeitung von Protokolldaten, der an zentraler Stelle sämtliche Protokolldaten speichert und sie dem Zugriff von den Produktionsmaschinen aus und durch deren Administratoren entzieht.
5. Auf alle schon getroffenen Maßnahmen sind ihrerseits technische und organisatorische Maßnahmen anzuwenden, um die Wirksamkeit, die Zuverlässigkeit, die Robustheit, die Belastbarkeit und die Evaluierbarkeit der Maßnahmen zu verbessern und ihre Rechtmäßigkeit sicherzustellen.
   Das folgende Beispiel verdeutlicht die Strategie der Selbstanwendung der Maßnahmen auf sich selbst. Transparenz bedeutet, dass eine Verarbeitungstätigkeit anhand von Soll-Ist-Bilanzen prüfbar sein muss. Prüfbarkeit im Nachhinein bedeutet, dass Protokolldaten erzeugt, gespeichert und verarbeitet werden müssen. Die Protokolldaten müssen dann durch zusätzliche

Maßnahmen revisionsfest gespeichert und deren Vertraulichkeit gewährleistet sein, indem sie signiert und verschlüsselt übertragen und gespeichert werden.

Zu beachten ist, dass neue Risiken durch ergriffene technische und organisatorische Maßnahmen entstehen können. Diese Risiken sind zu bewerten und angemessen zu reduzieren. Als Beispiel kann eine Vollprotokollierung von Mitarbeiter-Handlungen gefordert sein, die zugleich das Risiko birgt, dass durch Auswertungen dieses Protokolls eine unzulässige Leistungs- und Verhaltenskontrolle stattfindet. Wird in diesem Schritt eine Verarbeitung so verändert, dass die getroffenen Maßnahmen zu neuen Risiken, die höher sind als das Ausgangsrisiko, und somit zu einer Erhöhung des Schutzbedarfs führen, muss die Ausgestaltung der Maßnahmen erneut evaluiert werden. Die oben genannten Strategiensind in einem iterativen Prozess so lange anzuwenden, bis die Ausgestaltung der Maßnahmen ein angemessenes Schutzniveau gewährleistet.

D4 Datenschutzmanagement mit dem Standard- Datenschutzmodell

Das Datenschutzmanagement ist eine umfassende Methode, um systematisch alle Anforderungen des Datenschutzrechts in einer Organisation umzusetzen. Im Folgenden wird ein Datenschutzmanagement im Zusammenspiel mit dem SDM näher beschrieben.

D4.1 Rechtliche Grundlagen des Datenschutzmanagements

Der Verantwortliche ist für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich und muss den Nachweis darüber erbringen können. Konkret muss der Verantwortliche gemäß Art. 30 DS-GVO ein Verzeichnis führen, in dem die personenbezogenen Verarbeitungstätigkeiten der Organisationen aufgelistet sind. Zudem muss er bereits zum Zeitpunkt der Festlegung der Mittel geeignete technische und organisatorische Maßnahmen treffen (Art. 25 Abs. 1 DS-GVO - Datenschutz durch Technikgestaltung). Für Verarbeitungstätigkeiten, die ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, muss er gemäß Art. 35 DS-GVO darüber hinaus eine Datenschutz-Folgenabschätzung (DSFA) durchführen. Um zu beurteilen, ob von einer Verarbeitungstätigkeit ein voraussichtlich hohes Risiko ausgeht und demnach die Durchführung einer DSFA erforderlich ist, muss für jede Verarbeitung eine Schwellwertanalyse durchgeführt werden. Auch ohne DSFA müssen geeignete technische und organisatorische Maßnahmen bestimmt und dauerhaft umgesetzt werden, um ein dem Risiko angemessenes Schutzniveau bei jeder Verarbeitung personenbezogener Daten zu gewährleisten. Schließlich muss der Verantwortliche die Umsetzung und die Wirksamkeit der Maßnahmen nachweisen, evaluieren und ggf. verbessern können und auf diese Weise aktuell halten.

Damit der Verantwortliche den detaillierten Anforderungen in Bezug auf die operative Umsetzung der Betroffenenrechte und seinen Rechenschafts- und Nachweispflichten (vgl. Abschnitt B1.8) nachkommen kann, ist eine systematische Vorgehensweise bei der Prüfung und Beurteilung erforderlich, die sich sowohl auf jede einzelne Verarbeitungstätigkeit als auch auf sämtliche Verarbeitungstätigkeiten mit Personenbezug der gesamten Organisation und die dazu gehörigen technischen und organisatorischen Maßnahmen bezieht. Diese Rechenschafts- und Nachweispflichten sind eine dauerhafte Aufgabe für den Verantwortlichen und sollte daher als dauerhafter, zyklischer Prozess etabliert werden. Mit dem aus dem Qualitätsmanagement bekannten und bewährten PDCA-Zyklus (Plan, Do, Check, Act) steht ein kontinuierlicher Verbesserungsprozess in vier Phasen zur Verfügung, der die Grundlage für den hier beschriebenen Datenschutzmanagement-Prozess (DSM-Prozess) bildet. Der DSM-Prozess dient somit einerseits dem Verantwortlichen bei der systematischen Planung, dem dauerhaften Betrieb, der regelmäßigen Überprüfung der Datenschutzkonformität und

der Verbesserung von Verarbeitungstätigkeiten. Er schafft somit Transparenz für den Verantwortlichen. Andererseits hilft der DSM-Prozess auch den Datenschutzaufsichtsbehörden bei der Beratung von Verantwortlichen und bei der datenschutzrechtlichen Prüfung dieser Verarbeitungstätigkeiten, da die Datenschutzprüfungen der Aufsichtsbehörden in der Regel diesem Prozess-Ablauf entsprechen.

D4.2 Vorbereitungen

Vor dem Start des DSM-Zyklus sind ebenso wie vor der Anwendung des SDM [5)] die folgenden drei Voraussetzungen zu klären:

1. Klarheit über die sachlichen Verhältnisse, im Rahmen derer die zu betrachtende Datenverarbeitung stattfindet oder stattfinden soll.
2. Prüfung der Zulässigkeit der Verarbeitung. [6)]
3. Weitere materiellrechtliche Beurteilungen der Rechtmäßigkeit dieser Verarbeitung.

Zur Feststellung der sachlichen Verhältnisse beim Verantwortlichen der Verarbeitungstätigkeit sind beispielsweise folgende Fragen zu klären:

- Welche Stellen sind an der Verarbeitung beteiligt?
- Wer trägt für welche Teile der Verarbeitung die Verantwortung?
- Welche Geschäftsprozesse des Verantwortlichen werden durch die Verarbeitung unterstützt?
- Welche Daten werden in welchen Schritten und unter Nutzung welcher Systeme und Netze verarbeitet?
- Welche Personen nehmen die Datenverarbeitung vor und durch welche Personen erfolgt eine Kontrolle?
- Welche Hilfsprozesse werden zur Unterstützung der Verarbeitungstätigkeit betrieben?

Im Rahmen der Prüfung der Zulässigkeit der Verarbeitung ist die Rechtsgrundlage für die Verarbeitung zu bestimmen. Dazu können bei der Verarbeitung personenbezogenen Daten [7)] insbesondere die folgenden aus Art. 6 Abs. 1 DS-GVO abgeleiteten Fragen herangezogen:

- Bilden Einwilligungen der Betroffenen die Rechtsgrundlage der Verarbeitungstätigkeit?
- Ist die Verarbeitung für die Erfüllung eines Vertrags erforderlich, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen?
- Ist die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt?
- Ist die Verarbeitung erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen?
- Ist die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde?
- Ist die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich? Überwiegen dabei die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt?

Die materiellrechtliche Bewertung beurteilt, inwieweit die vom Verantwortlichen geplante und gegebenenfalls von der Aufsichtsbehörde zu prüfende Verarbeitungstätigkeit grundsätzlich zulässig

ist. Darüber hinaus gibt sie Antworten insbesondere auf die folgenden Fragen, die die Anwendung des SDM vorbereiten:

- Welches nationale Datenschutzrecht ist auf die Verarbeitung anzuwenden?
- Welche legitimen Zwecke können mit der Verarbeitung verfolgt werden und welche

Zweckänderungen sind im Zuge der Verarbeitung zulässig?

- Welche Daten sind für die Erfüllung der zulässigen Zwecke erheblich und erforderlich?
- Welche Rechtsgrundlagen bestehen zur Übermittlung von Daten an Personen innerhalb und außerhalb der beteiligten Stellen sowie von diesen an Dritte?
- Sind die erforderlichen Vereinbarungen getroffen, wenn mehrere Verantwortliche in die Verarbeitungstätigkeit involviert sind und gemeinsam verantwortlich sind (Art. 26 DS-GVO)?
- Sind Auftragsverarbeiter in die Verarbeitung involviert und sind die

Rechtsverhältnisse zwischen ihnen geregelt (Art. 28 DS-GVO)?

- Welchen, auf den Einzelfall bezogenen, besonderen Anforderungen müssen die technischen und organisatorischen Maßnahmen genügen?

Ausführlichkeit und Detaillierungsgrad insbesondere der Feststellungen zu den sachlichen Verhältnissen werden von Verarbeitung zu Verarbeitung variieren, ebenso wie der Grad der Formalisierung des Vorgehens von informeller Befragung bis hin zum Einsatz von standardisierten Fragebögen. Eine strukturierte Zusammenfassung der Ergebnisse ist unabhängig davon ebenso üblich wie für die weiteren Schritte unentbehrlich. Die Feststellungen zu den sachlichen Verhältnissen gehen in die Phase 1 „Planen/Spezifizieren“ des DSM-Zyklus ein.

D4.3 Spezifizieren und Prüfen

Grundlegende Voraussetzung für ein Spezifizieren (siehe Abschnitt D4.5.1) und ein späteres Prüfen (siehe Abschnitt D4.5.3) ist die Festlegung, wie die Gewährleistungsziele für die betrachtete Datenverarbeitung operationalisiert werden.

- In Abhängigkeit vom festgestellten Risiko (siehe dazu auch Abschnitt D3) und unter Bezug auf die konkreten rechtlichen Anforderungen sind die aus den jeweiligen Gewährleistungszielen resultierenden Eigenschaften der Verarbeitungstätigkeit qualitativ näher zu bestimmen: **Verfügbarkeit** *Innerhalb von welchen Prozessen ist für wen die Verfügbarkeit von welchen Daten zu gewährleisten? Innerhalb welcher Zeiten müssen Daten für wen verfügbar und ggf. wiederherstellbar sein?* Der Einfluss der ordnungsgemäßen Verwendung der Daten auf die Interessen der Betroffenen ist der Maßstab für die Konkretisierung des Gewährleistungsziels der Verfügbarkeit.
- **Integrität** *Welche Daten sind auf eine identifizierte oder identifizierbare Person bezogen und müssen daher unversehrt und aktuell gehalten werden?* Wie wird sichergestellt, dass die Prozesse, Systeme und Dienste dem gesetzten Zweck entsprechend korrekt geplant, betrieben und kontrolliert werden? Auch hier ist das Interesse der Betroffenen der Maßstab.
- **Vertraulichkeit** *Wem ist die Kenntnisnahme welcher Daten zu verwehren? Welche Prozesse, Systeme und Dienste sind potentiell für unbefugte Zugriffe anfällig?* Das Ausmaß des befugten Zugriffs ist zunächst technikunabhängig aus den jeweiligen Geschäftsprozessen abzuleiten. Hiermit ist der Rahmen bestimmt, innerhalb dessen sich die Maßnahmen zum Vertraulichkeitsschutz gegenüber unbefugten Beschäftigten des Verantwortlichen zu bewegen haben. Der Rahmen für die Kenntnisnahme Dritter ist durch die in der materiell-rechtlichen

Analyse festgestellten Übermittlungsbefugnisse gegeben.

- **Transparenz** *Wie und in welcher Form ist die Datenverarbeitung gegenüber betroffenen Personen und Aufsichtsbehörden transparent zu halten?* Es sind Anforderungen an die Informations- und Auskunftspflichten gemäß Art. 12 ff DS- GVO, die Benachrichtigungspflicht nach Art. 34 DS-GVO, an die Dokumentation der Verarbeitung nach Art. 30 DS-GVO, an die interne Dokumentation der Verarbeitungsvorgänge und deren Auswertbarkeit sowie an die Revisionsfähigkeit der Verarbeitung festzuhalten.
- **Intervenierbarkeit** *In welcher Ausprägung sind Betoffenenrechte zu gewähren?* Es muss festgelegt werden, wie betroffene Personen ihre Rechte wahrnehmen können, wie sichergestellt wird, dass Anfragen berechtigt stattfinden, wie in die Verarbeitung personenbezogener Daten eingegriffen werden kann (z. B. durch Berichtigung, Löschung oder Einschränkung der Verarbeitung von personenbezogenen Daten) und in welche Form Daten von oder zu anderen Verantwortlichen übertragen werden können.
- **Nichtverkettung** *Welche Zweckänderungen sind zulässig? Welche Zwecke von Hilfsprozessen leiten sich aus den Kernprozessen legitim ab?* Benötigt werden lediglich Aussagen zu solchen Zwecken, welche die Verantwortlichen tatsächlich verfolgen bzw. zu verfolgen beabsichtigen. Maßnahmen zur Gewährleistung der Nichtverkettung sollen mit dem Ziel ergriffen werden, die Verarbeitung oder Nutzung der Daten für alle außer den festgelegten legitimen Zwecken auszuschließen.
- **Datenminimierung** *Auf welche Weise wird das Gebot der Datenminimierung umgesetzt?* Es ist zu klären, wie die Kenntnisnahme von und die Ausübung welcher Verfügungsgewalt über welche Daten der Betroffenen durch welche Personen und Stellen zu minimieren sind. Dazu gehört es auch Speicherfristen für personenbezogene Daten sowie Prozesse zur Sicherstellung ihrer Einhaltung festzulegen. Ausgangspunkt sind dabei erneut die Interessen der Betroffenen, auch innerhalb einer Verarbeitung zu legitimen Zwecken die Belastung auf das erforderliche Maß zu begrenzen.
- **Belastbarkeit** *Sind Systeme und Prozesse auf Ereignisse, welche Störungen der regulären Abläufe verursachen, hinreichend vorbereitet?* Es ist zu klären, welche Schadensereignisse, Störungen oder Angriffe negative Auswirkungen für Betroffene haben können und ob hierfür Gegenmaßnahmen zur Verfügung stehen und diese zielgerichtet und zeitnah angewandt werden können. Aufgrund des Querschnittscharakters des Ziels der Belastbarkeit kann davon ausgegangen werden, dass bei einem hohen Reifegrad der Umsetzung der übrigen Gewährleistungsziele ein hinreichender Grad an Belastbarkeit erreicht ist.

Nachdem die Gewährleistungsziele bzgl. der Verarbeitungstätigkeit qualitativ konkretisiert wurden, können technische und organisatorische Maßnahmen bestimmt werden. Zu diesem Zweck werden die Ergebnisse der Datenschutzfolgen-Abschätzung herangezogen, sofern eine durchgeführt wurde. Das im Rahmen der Risikobeurteilung festgestellte Risiko für die Rechte und Freiheiten der von der Verarbeitung Betroffenen ist maßgeblich für das weitere Vorgehen. Ihr Ergebnis fließt in dreierlei Form in die weiteren Betrachtungen ein.

Zum Ersten können die Gewährleistungsziele quantitativ näher bestimmt werden. Beispiele für Präzisierungen sind Antworten auf folgende Fragen: Für welchen Zeitraum ist der Verlust der Verfügbarkeit der Daten für die Betroffenen in welchem Grad tolerabel? Mit welcher Verzögerung soll die Aktualität der Daten garantiert werden? Mit welcher zeitlichen Präzision muss die Verarbeitung im Nachhinein nachvollzogen werden können? In welchem zeitlichen Rahmen muss der Verantwortliche in der Lage sein, die jeweiligen Betroffenenrechte zu gewähren? Wie lange dürfen Daten zu welchen Zwecken verarbeitet werden, bevor diese von der Verarbeitung ausgeschlossen oder gelöscht werden?

Zum Zweiten bildet das Ergebnis der Risikoprüfung bzw. der Datenschutz-Folgenabschätzung die

Grundlage für die Abwägung zwischen der Wahrung der Interessen der Betroffenen und dem hierfür erforderlichen Aufwand des Verantwortlichen. Für übliche Verarbeitungskontexte ist das Ergebnis einer solchen Abwägung durch die Darstellung typischer Referenzmaßnahmen in Kapitel D1 vorgezeichnet.

Zum Dritten fließt das Ergebnis der Datenschutz-Folgenabschätzung in die Bewertung der Restrisiken ein, die nach Umsetzung der Maßnahmen verbleiben, die mit einem Aufwand ergriffen werden können, der in angemessenem Verhältnis zum Zweck der Verarbeitung besteht. Diese Risiken können von dem Interesse Dritter oder Beteiligter abhängen, die Gewährleistungsziele zu verletzen, sei es um Daten der Betroffenen unbefugt zur Kenntnis zu nehmen, um sie für illegitime Zwecke, über das erforderliche Maß hinaus oder in intransparenter Weise zu verarbeiten.

D4.4 Datenschutzmanagement-Prozess

Ausgehend von den Vorbereitungen (siehe Abschnitt D4.2) kann bestimmt werden, in welcher Ausprägung die Gewährleistungsziele (siehe Abschnitt D4.3) anzuwenden und zu betrachten sind.

Der DSM-Prozess (siehe Abbildung 1) wird in Anlehnung an den bewährten PDCA-Zyklus ausgestaltet. Der Datenschutz-PDCA-Zyklus (DSM-Zyklus) umfasst die folgenden vier Phasen:

- Plan: Planen und Spezifizieren / DSFA / Dokumentieren
- Do: Implementieren / Protokollieren
- Check: Kontrollieren / Prüfen / Beurteilen
- Act: Verbessern

Das SDM unterstützt den Verantwortlichen bei der Durchführung von Schwellwertanalyse und Datenschutz-Folgenabschätzung und der daraus resultierenden Auswahl eines Satzes von technischen und organisatorischen Maßnahmen (Soll-Werte), indem individuell gewählte Maßnahmen mit den generischen Maßnahmen (vgl. Abschnitt D1) und den im Referenzmaßnahmen-Katalog vorgeschlagenen Maßnahmen abgeglichen werden (in **Phase 1** des DSM-Zyklus). Die ausgewählten Maßnahmen werden in **Phase 2** für den laufenden Betrieb umgesetzt. Die aus der Planungsphase resultierenden funktionalen Soll-Werte werden mit den aus dem laufenden Betrieb resultierenden funktionalen Ist-Werten verglichen (**Phase 3a**). Anschließend erfolgt eine Beurteilung der Erfüllung der rechtlichen Vorgaben und der ggf. verbleibenden Restrisiken für die Rechte und Freiheiten der Betroffenen (**Phase 3b**). Ein zu geringes Schutzniveau bzw. als zu hoch beurteilte Restrisiken müssen dann durch entsprechende Verbesserungen etwa durch zusätzliche Maßnahmen auf ein akzeptables Maß gemindert werden (**Phase 4**).

Die zum Ende von Phase 3 getroffene Beurteilung kann in der Folge sowohl Grundlage für die Empfehlung bzw. die Aufforderung der Aufsichtsbehörde als auch der Anweisungen des Verantwortlichen bilden, entweder durch zusätzliche technische oder organisatorische Maßnahmen die Defizite zu beheben oder von der Verarbeitungstätigkeit Abstand zu nehmen, soweit sich die Rechtskonformität nicht herstellen oder eine ausreichende Risikominderung mit verhältnismäßigen Mitteln nicht erreichen lässt (Phase 4 des DSM- Zyklus).

Die nachfolgende Grafik zeigt den gesamten DSM-Zyklus, in den das SDM eingebunden ist.

Abbildung 1: Der PDCA-Zyklus des Datenschutzmanagements (DSM-Zyklus) als Rahmen für die

Anwendung des Standard- Datenschutzmodells bei Planungs-, Beratungs- und Prüfvorgänge

Für jede Verarbeitungstätigkeit wird es in der Regel erforderlich sein, den DSM-Zyklus mehrfach zu durchlaufen. Das betrifft insbesondere den Verantwortlichen bei der Planung von Verarbeitungstätigkeiten. So könnte bei der Inbetriebnahme eines Fachverfahrens ein erster Zyklus dessen Testbetrieb betreffen, der zweite Zyklus den Pilotbetrieb und der dritte Zyklus den Wirkbetrieb. Die Häufigkeit der Durchläufe hängt davon ab, wie weit der Verarbeitungskontext an die Erfordernisse des Datenschutzes in der Planungsphase oder im Rahmen eines Prüfprozesses der Aufsichtsbehörde angepasst werden musste.

D4.4.1 Plan: Spezifizieren / DSFA / Dokumentieren

In Phase 1 zur Planung einer Verarbeitungstätigkeit mit Personenbezug werden angemessene Maßnahmen bestimmt, durch die die Risiken des Grundrechtseingriffs gemildert, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann. Um den Nachweis der Wirksamkeit der Maßnahmen erbringen zu können, müssen funktionale Anforderungen (Soll-Werte) festgelegt und dokumentiert werden. Diese werden aus den gesetzlichen Anforderungen (Soll) hergeleitet (siehe Teil B Anforderungen der DS-GVO). Erst dann wird festgelegt, welche Aktivitäten der Programme und Systeme und welche Ereignisse von Prozessen zu protokollieren sind.

Eine wesentliche Komponente der Phase 1 ist die Durchführung einer Schwellwert-Analyse und eine daraus ggfs. resultierende Datenschutz-Folgenabschätzung (DSFA).

Eine DSFA ist durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat. Ob ein voraussichtlich hohes Risiko durch eine Verarbeitungstätigkeit mit Personenbezug besteht, ist vorher im Rahmen einer obligatorischen Schwellwert-Analyse festzustellen (siehe Teil D3.2.1). Ein Ergebnis der DSFA ist der DSFA-Bericht, in dem die Risiken aufgezeigt und die Funktionen und technischen und organisatorischen Maßnahmen zur Verringerung von Risiken bestimmt werden. Häufig werden in diesem Bericht zusätzlich Empfehlungen zur weiteren Vorgehensweise bei der Implementierung der zu ergreifenden Maßnahmen angegeben, weil Art. 35 DS-GVO die Implementierung von solchen Abhilfemaßnahmen fordert.

Der Verantwortliche muss während der Phase 1 über die DSFA entscheiden. Am Ende der Phase 1 entscheidet er über die geplante Implementierung der Funktionen und der technischen und organisatorischen Maßnahmen.

Die Durchführung einer DSFA ist dabei kein einmaliger Vorgang. Sollten sich wesentliche Änderungen im Verfahren oder bei den Umständen der Verarbeitung , die die Bewertung bereits erkannter Risiken ändern, oder neue Risiken bekannt werden, so ist die DSFA zu überprüfen und anzupassen. Um dies zu garantieren, wird ein stetiger, iterativer Prozess der Überprüfung und Anpassung von Funktionen empfohlen. Dieser iterative Prozess der DSFA ist in den DSM-Prozess eingebunden.

Die Implementierung der empfohlenen Funktionen und der technischen und organisatorischen Maßnahmen geschieht in Phase 2 des DSM.

Weitere Details zur systematischen Durchführung einer Datenschutz-Folgenabschätzung können dem Kurzpapier Nr. 5 der Datenschutzkonferenz entnommen werden. [8)]

D4.4.2 Do: Implementieren / Protokollieren

In Phase 2 werden die aus den Ergebnissen der Phase 1 empfohlenen Maßnahmen entsprechend den Anweisungen des Verantwortlichen umgesetzt. Auf der Basis der Dokumentation der funktionalen Soll-Werte werden Aktivitäten von IT-Systemen und Administratoren und welche Ereignisse prüffähig dokumentiert und protokolliert. Beim Vorliegen eines DSFA-Berichts muss der Verantwortliche dessen Ergebnisse bei der Implementierung von Verarbeitungstätigkeiten berücksichtigen.

Bei der Implementierung von Systemen und Programmen ist darauf zu achten, dass anhand von System-Dokumenten und Protokollen die Funktionen der Fachapplikationen und der Schutzvorkehrungen von IT-Systemen und Diensten auf den verschiedenen Ebenen (Client, Server) überprüft werden können. Das Vorliegen dieser Dokumente und Protokolle (Ist- Werte) ist die Voraussetzung zur Durchführung der Phase 3 des DSM.

D4.4.3 Check: Kontrollieren, Prüfen Beurteilen

Der Kern der Anwendung des SDM im DSM-Zyklus besteht darin, die in der Planungsphase bestimmten funktionalen Soll-Werte mit den festgestellten Ist-Werten in Beziehung zu setzen (Phase 3a). Zudem werden die relevanten Referenzmaßnahmen mit den tatsächlich umgesetzten technischen und organisatorischen Maßnahmen verglichen. Abweichungen vom Soll sind danach zu beurteilen, inwieweit sie die Umsetzung der Grundsätze aus Artikel 5 DS-GVO bzw. das Erreichen der Gewährleistungsziele gefährden. In einem Prüfvorgang der Aufsichtsbehörde erlaubt die bis zu diesem Punkt geführte Analyse aus einem Verfehlen der Gewährleistungsziele auf (ggf. sanktionierbare) datenschutzrechtliche Mängel zu schließen.

In der Prüf- und Beurteilungspraxis lässt sich häufig mit nur geringem Aufwand feststellen, ob Anforderungen nicht erfüllt werden, weil die entsprechend zugeordneten Maßnahmen fehlen, Maßnahmen falsch oder unzureichend umgesetzt sind oder die Referenzmaßnahmen nicht korrekt angewendet wurden. Komplizierter ist der Fall, wenn die zu prüfende Stelle andere als die Maßnahmen des Referenzmaßnahmen-Katalogs gewählt hat. Auch wenn diese als grundsätzlich geeignet beurteilt werden können, muss separat geprüft werden, ob sie in ihrer konkreten Ausgestaltung tatsächlich dem festgestellten Risiko entsprechen. An dieser Stelle hilft das SDM, die Erörterung auf den Nachweis dessen zu fokussieren, dass (oder inwieweit) die getroffene technische oder organisatorische Maßnahme funktional äquivalent bzw. wirkungsgleich zur Referenzmaßnahme ist.

Ausgangspunkt für die datenschutzrechtliche Beurteilung einer Verarbeitungstätigkeit ist die Feststellung der funktionalen Soll-Ist-Differenzen. Diese Differenzen werden in der Beurteilungsphase (Phase 3b) wieder ins Rechtliche übersetzt und mit den datenschutzrechtlichen Anforderungen (Soll) verglichen. Im Rahmen einer datenschutzrechtlichen Beurteilung werden aus den festgestellten Abweichungen ggfs. „normative Mängel“. Je gravierender ein Mangel ist, umso wirksamer muss er durch entsprechende Änderungsanweisungen in Phase 4 des DSM-Prozesses für ein erneutes Durchlaufen aller Phasen des DSM-Zyklus abgestellt werden. Das Ergebnis der Phase 3b besteht in Beurteilungen, die geeignet sind, um rechtliche und funktionale Verbesserungen herbeizuführen.

D4.4.4 Act: Verbessern und Entscheiden

Die in Phase 3b festgestellten Mängel müssen so formuliert sein, dass anschließend konkrete

funktionale Maßnahmen getroffen werden können. Diese Beurteilungen als Ergebnisse aus Phase 3 sind vom Verantwortlichen in Phase 4 zu sichten, zu beraten und zu priorisieren. In dieser Phase 4 müssen festgestellte Mängel zu Entscheidungen des Verantwortlichen und daraus resultierenden Anweisungen zu Änderungen von Maßnahmen oder zu neuen Maßnahmen führen, die dann im einen neuen Zyklus zu planen, zu implementieren und zu prüfen sind. Wurden Maßnahmen getroffen, die alle Mängel beseitigen, kann davon ausgegangen werden, dass alle Defizite beseitigt wurden und die Verarbeitungstätigkeit rechtskonform ist.

---

1) https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf, Stand: 26.04.2018, letzter Aufruf: 29.07.2019.

2) Diese Definition des Risikos kann aus den ErwGr 75 DS-GVO hergeleitet werden.

3) Dieses Arbeitspapier wurde ursprünglich durch die Vorgängerinstitution des EDSA, die Artikel-29-Arbeitsgruppe, und später durch den EDSA mit Bestätigung 1/2018 angenommen. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, Stand: 13.10.2017 (Revision 0.1; letzter Aufruf: 01.04.2019) (aus: WP 248 der Art. 29 Gruppe, ab Seite 10 f)

4) https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf, Stand: 26.04.2018, letzter Aufruf: 01.04.2019.

5) S. hierzu bereits Fn. 5.

6) Zur Differenzierung zwischen Zulässigkeit und Rechtmäßigkeit s. Kapitel A1.

7) Werden besondere Kategorien personenbezogener Daten verarbeitet, ist zudem Art. 9 DS-GVO zu beachten.

8) https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf, Stand: 26.04.2018, letzter Aufruf: 01.04.2019.