Das Standard-Datenschutzmodell

Eine Methode zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele

V.1.0 – Erprobungsfassung

von der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 9. und 10. November 2016 in Kühlungsborn einstimmig zustimmend zur Kenntnis genommen (Enthaltung durch Freistaat Bayern)

Inhalt

1 Einleitung

Die Europäische Datenschutz-Grundverordnung (2016/679/EU-DS-GVO) ist am 25. Mai 2016 in Kraft getreten und gilt nach einer zweijährigen Übergangsfrist unmittelbar in der gesamten Europäischen Union. Die DS-GVO enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. In den Art. 5, 12, 25und 32 finden sich grundlegende Anforderungen an die Sicherheit der Verarbeitung personenbezogener Daten. Die Verordnung fordert geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1). Zudem fordert die DS-GVO ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 Satz 1 lit. d). Zur Bewertung von IT-gestützten Verfahren sind Verhaltensregeln festgelegt und Zertifizierungen werden möglich (Art. 40-43 DS-GVO). Schließlich sieht die DS-GVO ein Kohärenzverfahren vor, das die unabhängigen Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet (Kapitel VII –Zusammenarbeit und Kohärenz). Dieses Verfahren erfordert ein abgestimmtes, transparentes und nachvollziehbare System zur datenschutzrechtlichen Bewertung der Verarbeitung personenbezogener Daten.

In Art. 5 der DS-GVO werden wesentliche Grundsätze für die Verarbeitung personenbezogener Daten formuliert: Die Verarbeitung muss rechtmäßig, nach Treu und Glauben, nachvollziehbar, zweckgebunden, auf das notwendige Maß beschränkt, auf der Basis richtiger Daten, vor Verlust, Zerstörung und Schädigung geschützt und die Integrität und Vertraulichkeit wahrend stattfinden. Das *Standard-Datenschutzmodell (SDM)* bietet geeignete Mechanismen, um diese rechtlichen Anforderungen der DS-GVO in technische und organisatorische Maßnahmen zu überführen. Zu diesem Zweck strukturiert das SDM die rechtlichen Anforderungen in Form der Gewährleistungsziele Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung und Intervenierbarkeit. Mit Hilfe dieser Gewährleistungsziele überführt das SDM die rechtlichen Anforderungen des DS-GVO in den von der Verordnung geforderten Katalog von technischen und organisatorischen Maßnahmen. Dieser Referenzkatalog ermöglicht zudem, die Maßnahmen auf ihre Wirksamkeit zu überprüfen. Derartig standardisierte Maßnahmenkataloge bieten zudem eine sehr gut geeignete Grundlage für die von der DS-GVO geförderten datenschutzspezifischen Zertifizierungen.

Eine derartige Standardisierung unterstützt somit auch die in der Verordnung normierte Zusammenarbeit der Aufsichtsbehörden. Denn auch auf nationaler Ebene müssen die deutschen Datenschutzbehörden in zunehmendem Maße zusammen arbeiten und mit einheitlichen Beratungs- und Prüfkonzepten die modernen Verfahren zur automatisierten Verarbeitung personenbezogener Daten begleiten. Das SDM als ganzheitliches Prüf- und Beratungskonzept kann dabei zu einem abgestimmten, transparenten und nachvollziehbaren System der datenschutzrechtlichen Bewertung führen.

Das SDM kann darüber hinaus auch dazu beitragen, die vom IT-Planungsrat verabschiedete Nationale E-Government-Strategie (NEGS) datenschutzkonform umzusetzen. Am 18. Oktober 2015 hat der IT-Planungsrat die Fortschreibung der NEGS beschlossen, mit der sich Bund, Länder und Gemeinden gemeinsam darauf verständigt haben, wie die elektronische Abwicklung von Verwaltungsangelegenheiten über das Internet weiterentwickelt werden soll. Einer der Leitgedanken, an dem Bund und Länder sich im gemeinsamen wie auch in ihrem jeweils eigenen Handeln im E-Government ausrichten, betrifft Fragen der Informationssicherheit und des Datenschutzes. Die NEGS stellt klar, dass E-Government sicher und datenschutzgerecht sein muss, wenn es das uneingeschränkte Vertrauen der Bürger und Unternehmer in das elektronische Verwaltungshandeln erringen und behalten will. Es werden technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes gefordert, die den Grundsatz der Datenminimierung wahren und die sich auf die Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit beziehen sollen. Das SDM basiert auf diesen Zielen und ist als Werkzeug zur Umsetzung der Datenschutzziele der NEGS hervorragend geeignet.

Das hier beschriebene Standard-Datenschutzmodell kann somit in Deutschland und auch im internationalen Kontext sowohl für die Datenschutzaufsicht im Bereich der privaten Wirtschaft und im Bereich der öffentlichen Verwaltung als auch für die verantwortlichen Stellen in beiden Bereichen einen wesentlichen Beitrag leisten, um einen an Grundrechten orientierten Datenschutz durchzusetzen. Denn das SDM ermöglicht einerseits einen systematischen und nachvollziehbaren Vergleich zwischen Soll-Vorgaben, die sich aus Normen, Verträgen, Einwilligungserklärungen und Organisationsregeln ableiten, und andererseits die Umsetzung dieser Vorgaben sowohl auf organisatorischer als auch auf informationstechnischer Ebene in IT-Verfahren und -Systemen.

Mit dem SDM wird *eine* Methode bereitgestellt, mit dem die Risiken für das Recht auf informationelle Selbstbestimmung, die mit der Verarbeitung personenbezogener Daten zwangsläufig einhergehen, mit Hilfe von geeigneten technischen und organisatorischen Maßnahmen beseitigt oder wenigstens auf ein tragbares Maß reduziert werden können. Für das Erstellen von Datenschutz- und Sicherheitskonzepten sind neben derartigen Methoden und Hilfsmitteln aber auch die langjährigen, individuellen Erfahrungen der handelnden Personen unerlässlich. Aus diesen Erfahrungen resultieren mitunter zwar dem SDM vergleichbare, im Detail aber abgewandelte Methoden zur Minimierung des Risikos. Diese Methoden können in speziellen Anwendungskontexten selbstverständlich ihre Berechtigung haben.

Das SDM wurde von den Aufsichtsbehörden in einer Phase des Umbruchs des europäischen Datenschutzrechts entwickelt. Die DS-GVO ist am 25. Mai 2016 in Kraft getreten, gilt unmittelbar aber erst nach einer Übergangsfrist von zwei Jahren. In diesem Übergangszeitraum gelten die herkömmlichen Datenschutzvorschriften wie das Bundesdatenschutzgesetz oder die Landesdatenschutzgesetze uneingeschränkt. Um die Anwendung des SDM auch in dieser Übergangszeit zu erleichtern, wird im nachfolgenden Text nicht nur die DS-GVO referenziert, sondern es werden ganz bewusst auch immer Bezüge zum BDSG hergestellt. Zum Ende der

Übergangsfrist im Mai 2018 wird das SDM in Bezug auf die dann geltenden rechtlichen Grundlagen überarbeitet.

2 Der Zweck des Standard-Datenschutzmodells

Die Verarbeitung personenbezogener Daten mit Hilfe informationstechnischer Verfahren ist datenschutzrechtlich danach zu beurteilen, ob sie auf einer ausreichenden Rechtsgrundlage erfolgt. Es gilt das Verbot mit Erlaubnisvorbehalt des § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) bzw. der entsprechenden Normen der Landesdatenschutzgesetze und künftig die Regelungen der DS-GVO, hier insbesondere die Verarbeitungsgrundsätze gem. Art. 5 und die Bedingungen für die Rechtmäßigkeit der Verarbeitung gem. Art. 6. Zudem ist zu prüfen, ob die Daten durch eine angemessene Auswahl technischer und organisatorischer Maßnahmen so verarbeitet werden, dass die Rechte der Betroffenen gewahrt bleiben (vgl. Anhang zu § 9 BDSG bzw. zukünftig insbesondere die Verarbeitungsgrundsätze gem. Art. 5 DS-GVO und die Bestimmungen zur Sicherheit der Verarbeitung gem. Art. 32). Das hier beschriebene SDM soll diese Maßnahmen auf der Basis von Gewährleistungszielen systematisieren.

Das Modell richtet sich einerseits an die für die Verarbeitung personenbezogener Daten verantwortlichen Stellen. Diese können mit dem SDM die erforderlichen Funktionen und Schutzmaßnahmen systematisch planen, umsetzen und kontinuierlich überwachen. Das Modell richtet sich zudem an die Datenschutzbehörden, um mit einer einheitlichen Systematik zu einem transparenten, nachvollziehbaren, belastbaren Gesamturteil über ein Verfahren und dessen Komponenten zu gelangen.

Ausgangspunkt der Analyse ist die Bestimmung der für die Verarbeitung verantwortlichen Stelle oder Stellen sowie des Zwecks der Verarbeitung im Kontext der mit dem Verfahren umgesetzten oder unterstützten Geschäftsprozesse und der relevanten Rechtsgrundlagen. Erst diese rechtlich zu erzielende Bestimmtheit ermöglicht es, die Funktionalität des Verfahrens einschließlich des erforderlichen Umfangs der Verarbeitung personenbezogener Daten und der angemessenen Schutzmaßnahmen entsprechend dem Stand der Technik festzulegen.

3 Der Anwendungsbereich des Standard-Datenschutzmodells

Der wesentliche Anwendungsbereich des Standard-Datenschutzmodells sind Planung, Einführung und Betrieb einzelner Verfahren, mit denen personenbezogene Daten verarbeitet werden (personenbezogene Verfahren) sowie deren Beurteilung durch die Datenschutzaufsichtsbehörden. Solche Verfahren sind dadurch gekennzeichnet, dass sie sich auf einen konkreten, abgrenzbaren und rechtlich legitimierten Verarbeitungszweck (im öffentlichen Bereich eine Ermächtigungsgrundlage) und auf die diesen Zweck verwirklichenden Geschäftsprozesse beziehen (siehe Kapitel 8).

Die Datenschutzgesetze des Bundes und der Länder fordern, für jede Verarbeitung personenbezogener Daten technische und organisatorische Maßnahmen auszuwählen und umzusetzen, die nach dem Stand der Technik und nach der Schutzbedürftigkeit der zu verarbeitenden Daten erforderlich und angemessen sind. Diese Datenschutzmaßnahmen werden als Teil des Verfahrens betrachtet, einschließlich der mit ihnen selbst möglicherweise verbundenen Verarbeitung personenbezogener Daten.

Die Rechtsgrundlage kann konkrete Maßnahmen vorschreiben, die verfahrensspezifisch umzusetzen sind, so z. B. eine Anonymisierung erhobener personenbezogener Daten, sobald ein bestimmter Zweck der Verarbeitung erreicht wurde. Außerdem kann es Fälle geben, in denen besondere Maßnahmen ergriffen werden müssen, die als Ergebnis einer gesetzlich erforderlichen Interessensabwägung rechtlich geboten sind.

In beiden Fällen stehen neben diesen verfahrensspezifisch ergriffenen Datenschutzmaßnahmen auch solche, die verfahrensübergreifend eingesetzt werden. Diese können z. B. auf die Verschlüsselung von Daten gerichtet sein, ihrer Integritätssicherung, der Authentisierung von Kommunikationspartnern und technischen Komponenten, der Protokollierung, der Pseudonymisierung und Anonymisierung oder dem Umgang mit Kontaktadressen für Beschwerden dienen oder als allgemeine Rollenkonzepte einen Rahmen für die Berechtigungsvergabe in verschiedenen Verfahren bieten.

Das SDM hat das Ziel, sowohl verpflichtende, wie auch optionale, sowohl verfahrensspezifische, als auch verfahrensübergreifende Datenschutzmaßnahmen zu systematisieren und ihre Bewertung zu ermöglichen.

Das SDM kann sowohl von den sechzehn Landesdatenschutzbeauftragten, dem Bayerischen Landesamt für Datenschutzaufsicht sowie der Bundesdatenschutzbeauftragte als auch von den verantwortlichen Stellen bei der Planung und beim Betrieb von Verfahren zur Verarbeitung personenbezogener Daten angewendet werden.

4 Die Struktur des Standard-Datenschutzmodells

Das Standard-Datenschutzmodell

- überführt datenschutzrechtliche Anforderungen in einen Katalog von Gewährleistungszielen,
- gliedert die betrachteten Verfahren in die Komponenten Daten, IT-Systeme und Prozesse,
- berücksichtigt die Einordnung von Daten in drei Schutzbedarfsabstufungen,
- ergänzt diese um entsprechende Betrachtungen auf der Ebene von Prozessen und IT-Systemen und
- bietet einen hieraus systematisch abgeleiteten Katalog mit standardisierten Schutzmaßnahmen (siehe Anhang).

5 Die Gewährleistungsziele

5.1 Der Begriff „Gewährleistungsziel“

Das SDM verwendet für die Beschreibung von bestimmten aus dem Datenschutzrecht resultierenden Kategorien von Anforderungen den Begriff „Gewährleistungsziel“. Diese Anforderungen zielen auf Eigenschaften normgerechter Verarbeitung, die durch technisch-organisatorische Maßnahmen "gewährleistet" werden müssen. Die Gewährleistung besteht im Ausschluss von Abweichungen. So ist eine Eigenschaft normgerechter Verarbeitung, dass sie nicht zu unberechtigter Kenntnisnahme führt. Die Maßnahmen müssen daher darauf abzielen, dass es zu unberechtigten Kenntnisnahmen nicht kommen kann. Die zu erreichende Zuverlässigkeit der Gewährleistung ist Gegenstand einer Abwägung zwischen Schutzbedarf (vgl. Kap. 8) und Aufwand unter Berücksichtigung des Stands der Technik. Die Verpflichtung, die Gewährleistungsziele durch technisch-organisatorische Maßnahmen zu erreichen, ist damit nicht absolut, sondern stets im Kontext der Umstände der Verarbeitung und der mit ihr verbundenen Risiken für die Rechte und Freiheiten der Betroffenen zu betrachten.

Zudem ist der Begriff „Gewährleistungsziel“ besonders gut geeignet, um den Bezug zum Urteil des Bundesverfassungsgerichts von 2008 (Urteil vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274) herzustellen. Das Bundesverfassungsgericht hatte seinerzeit das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abgeleitet (siehe auch Punkt 6.1).

Schließlich soll mit dieser Begriffswahl der Eindruck vermieden werden, dass durch das SDM der Katalog von Schutzzielen, der bereits in einigen Landesdatenschutzgesetzen enthalten ist, ohne Legitimation des Gesetzgebers ausgeweitet wird.

5.2 Die zentralen datenschutzrechtlichen Anforderungen

Die folgenden datenschutzrechtlichen Anforderungen, die übergreifend in allen deutschen Datenschutzgesetzen enthalten sind und deren Erfüllung Voraussetzung für die Rechtmäßigkeit einer personenbezogenen Datenverarbeitung bilden, werden vom Konzept der Gewährleistungsziele erfasst:

- die Zweckbindung einer Datenverarbeitung mit Personenbezug,
- die Begrenzung der Datenverarbeitung auf das erforderliche und datensparsame Maß,
- die Berücksichtigung der Betroffenenrechte, wonach in einem Verfahren Prozesse insbesondere für die Beauskunftung, die Korrektur, das Sperren und das Löschen von Betroffenendaten vorzusehen sind,
- die Transparenz von Verfahren als Voraussetzung dafür, dass die rechtlich festgelegten Anforderungen an ein Verfahren sowohl für die Organisation selber, als auch zumindest in einer allgemeinverständlichen Form für den Betroffenen sowie für die Aufsichtsbehörden überprüfbar sind,
- die Informationssicherheit der eingesetzten Komponenten zur Datenverarbeitung.

Das SDM betrachtet weder grundlegende Fragen der materiellen Rechtmäßigkeit eines Verfahrens noch spezialgesetzliche Regelungen oder Regelungen auf einem hohen Detaillierungsgrad (siehe Punkt 10). Die Orientierung an den allgemein geltenden Gewährleistungszielen des Datenschutzes erübrigt daher nicht die Kenntnisnahme der datenschutzrechtlichen Regelungen, auch nicht im Bereich der technisch-organisatorischen Schutzmaßnahmen.

5.3 Das grundlegende Gewährleistungsziel Datenminimierung

Allen Gewährleistungszielen ist gemein, dass sie bestimmen, welche Eigenschaften und Parameter von im Vorhinein als zulässig bestimmten Verarbeitungsvorgängen und Begleitprozessen zu wahren sind. Daher fordert der Gesetzgeber, den Datenstrom auf Wesentliches und auf ein notwendiges Maß beschränkend (Art. 5c DS-GVO) zu reduzieren, an der Quelle und jeder Verzweigung, im Vorhinein und – immer wichtiger im Zeitalter der mit dem Stichwort *Big Data* verknüpften explorativen Datenverarbeitung – im Zuge der Verarbeitung selbst. Diese grundlegende Anforderung erfasst in konzentrierter Form das Gewährleistungsziel der Datenminimierung, dessen Umsetzung daher einen durchgreifenden Einfluss auf Umfang und Intensität des durch die anderen Gewährleistungsziele bestimmten Schutzprogramms hat.

Datenminimierung konkretisiert und operationalisiert im Verarbeitungsprozess den Grundsatz der Erforderlichkeit, der von diesem Prozess insgesamt wie auch von jedem seiner Schritte verlangt, nicht mehr personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen, als für das Erreichen des Verarbeitungszwecks erforderlich ist. Datenminimierung ist als proaktives Element datenschutzfreundlicher Technikgestaltung zu berücksichtigen: beginnend beim Design der Informationstechnik durch den Hersteller, über ihre Konfiguration und

Anpassung an die Betriebsbedingungen, bis zu ihrem Einsatz in den Kernprozessen des Verfahrens wie auch in den unterstützenden Prozessen zum Beispiel bei der Wartung der verwendeten Systeme, von der Erhebung der personenbezogenen Daten über ihre Verarbeitung und Nutzung bis zur Löschung oder vollständigen Anonymisierung, über den vollständigen Lebenszyklus der Daten hinweg.

Die Verfolgung dieses Gewährleistungsziels setzt voraus, dass zunächst die Angemessenheit und Legitimität der Zwecksetzung sowie Erheblichkeit bzw. Erforderlichkeit der zu erhebenden Daten für die vorgesehenen Zwecke datenschutzrechtlich beurteilt worden sind, auf einer abstrakten Ebene, noch ohne Berücksichtigung prozeduraler und technischer Zwänge. Dies kann zu dem Ergebnis führen, dass auf die Verarbeitung von personenbezogenen Daten verzichtet werden kann und dann auch muss. Mit dieser Datenvermeidung ist das Optimum der Datenminimierung erreicht.

Ist eine vollständige Datenvermeidung nicht möglich, so können ausgehend von der als zulässig bewerteten Zwecksetzung und Datengrundlage Abfolgen von Verarbeitungsschritten bewertet werden,

- nach dem Umfang der verarbeiteten oder offengelegten Informationen,
- nach der Zahl der Stellen und Personen, welchen diese Informationen offenbart werden und
- nach dem Ausmaß der Verfügungsgewalt, den die jeweiligen Stellen und Personen über die Daten erlangen.

Das Gewährleistungsziel der Datenminimierung ist erreicht, wenn die Verarbeitung in diesen drei Dimensionen global im Zuge des gesamten Verarbeitungsprozesses und, in dessen Rahmen, lokal in jedem einzelnen Verarbeitungsschritt minimiert wird. Offensichtliche Beispiele von Parametern, die der Minimierung offenstehen, sind Datenfelder in Suchmasken und Schnittstellen oder Funktionen, die in menügesteuerten Systemen den Nutzern angeboten werden.

Der Grundsatz der Datenminimierung geht davon aus, dass der beste Datenschutz darin besteht, wenn keine oder möglichst wenige personenbezogene Daten verarbeitet werden. Datenminimierung als Gewährleistungsziel ist erreicht, wenn eine angemessene Annäherung an dieses Optimum erreicht ist. Das Optimierungsziel ist mit dem Bewertungskriterium der Minimierung von Verfügungsgewalt und Kenntnisnahme in den oben aufgeführten drei Dimensionen gegeben. An ihm orientiert kann die optimale Abfolge von Verarbeitungsschritten gewählt und in der Folge an sich verändernde Bedingungen angepasst werden. Im Laufe der Verarbeitung ist schließlich mit technischen und organisatorischen Maßnahmen zu gewährleisten, dass sich die Datenverarbeitung nur innerhalb des a priori gesteckten Rahmens bewegt.

Die frühestmögliche Löschung nicht weiter benötigter personenbezogener Daten ist eine solche Maßnahme, sicher die wichtigste und durchgreifendste. Zuvor jedoch können bereits

einzelne Datenfelder oder Attribute von bestimmten Formen der Verarbeitung ausgenommen oder die Zahl der Datensätze, auf die eine Funktionalität anwendbar ist, beschränkt werden. Datenfelder, welche die Bestimmung der Betroffenen ermöglichen, können gelöscht oder transformiert (Anonymisierung, Pseudonymisierung) oder ihre Anzeige in Datenmasken unterdrückt werden, so dass sie den handelnden Personen nicht zur Kenntnis gelangen, vorausgesetzt, diese Kenntnis ist für den Verarbeitungszweck entbehrlich.

5.4 Die elementaren Gewährleistungsziele

5.4.1 Die klassischen Gewährleistungsziele der Datensicherheit

Gewährleistungsziele spielen seit Ende der 1980er Jahre unter dem Begriff Schutzziele eine Rolle in der Gestaltung technischer Systeme, deren Sicherheit gewährleistet werden soll. Zu den „klassischen“ *Gewährleistungszielen der Datensicherheit* zählen:

1. Verfügbarkeit,
2. Integrität und
3. Vertraulichkeit.

(1) Das Gewährleistungsziel *Verfügbarkeit* bezeichnet die Anforderung, dass personenbezogene Daten zur Verfügung stehen müssen und ordnungsgemäß im vorgesehenen Prozess verwendet werden können. Dazu müssen sie im Zugriff von Berechtigten liegen und die vorgesehenen Methoden zu deren Verarbeitung müssen auf sie angewendet werden können. Das setzt voraus, dass die Methoden mit den vorliegenden Datenformaten umgehen können. Die Verfügbarkeit umfasst die konkrete Auffindbarkeit von Daten (z. B. mit Hilfe von Adressverzeichnissen, Geschäfts- oder Aktenzeichen), die Fähigkeit der verwendeten technischen Systeme, Daten auch für Menschen zugänglich angemessen darzustellen und die inhaltliche Interpretierbarkeit der Daten (ihre semantische Erfassbarkeit).

(2) Das Gewährleistungsziel Integrität bezeichnet einerseits die Anforderung, dass informations-technische Prozesse und Systeme die Spezifikationen kontinuierlich einhalten, die zur Ausübung ihrer zweckbestimmten Funktionen für sie festgelegt wurden. Integrität bezeichnet andererseits die Eigenschaft, dass die zu verarbeitenden Daten unversehrt, vollständig und aktuell bleiben. Abweichungen von diesen Eigenschaften müssen ausgeschlossen werden oder zumindest feststellbar sein, damit sie berücksichtigt bzw. korrigiert werden können. Versteht man das Gewährleistungsziel Integrität als eine Form der Richtigkeit im Sinne des Art, 5 Abs. 1 lit. d DS-GVO, resultiert daraus der Anspruch, dass zwischen der rechtlich-normativen Anforderung und der gelebten Praxis eine hinreichende Deckung besteht, sowohl in Bezug auf technische Details wie auch im großen Zusammenhang des Verfahrens und dessen Zwecksetzung insgesamt.

(3) Das Gewährleistungsziel *Vertraulichkeit* bezeichnet die Anforderung, dass keine Person personenbezogene Daten unbefugt zur Kenntnis nehmen kann. Unbefugte sind nicht nur Dritte außerhalb der verantwortlichen Stelle, mögen sie mit oder ohne kriminelle Absicht handeln, sondern auch Beschäftigte von technischen Dienstleistern, die zur Erbringung der

Dienstleistung keinen Zugriff zu personenbezogenen Daten benötigen, oder Personen in Organisationseinheiten, die keinerlei inhaltlichen Bezug zu einem Verfahren oder zu der oder dem jeweiligen Betroffenen haben.

Diese drei Gewährleistungsziele wurden von den verantwortlichen Stellen in den letzten Jahren in zunehmendem Maße in eigenem Interesse verfolgt, auch ohne dass hierfür gesetzliche Vorgaben vorlagen. Sie wurden zunächst ausschließlich für die IT-Sicherheit formuliert und beschreiben Anforderungen an einen sicheren Betrieb insbesondere von Verfahren durch Organisationen in Bezug auf ihre Geschäftsprozesse. Organisationen müssen ihre Geschäftsprozesse vor Angriffen schützen, unabhängig davon, ob sie von organisations-externen oder -internen Personen ausgeführt werden.

5.4.2 Auf den Schutz Betroffener ausgerichtete Gewährleistungsziele

Neben den aus der IT-Sicherheit bekannten Schutzzielen wurden aus bestehenden Datenschutz-Rechtsnormen weitere Gewährleistungsziele mit Datenschutzbezug entwickelt, aus denen technisch-organisatorische Maßnahmen abgeleitet werden. Auch aus datenschutzrechtlicher Sicht müssen Organisationen ihre Geschäftsprozesse vor Angriffen schützen, sofern personenbezogene Daten von den betrachteten Geschäftsprozessen berührt werden. Die Gewährleistungsziele des Datenschutzes erfordern in diesem Sinne im Vergleich zu den Gewährleistungszielen der IT-Sicherheit ein etwas erweitertes Verständnis, denn der Datenschutz nimmt zusätzlich eine darüber hinausgehende, erweiterte Schutz-Perspektive ein, indem er die Risiken betrachtet, die von den Aktivitäten der Organisation selbst innerhalb und außerhalb ihrer Geschäftsprozesse gegenüber betroffenen Personen ausgehen. Methodisch gesprochen muss sich deshalb nicht nur eine Person gegenüber einer Organisation durch überprüfbare Eigenschaften als vertrauenswürdig ausweisen, sondern auch eine Organisation gegenüber einer Person. Eine Datenschutzfolgenabschätzung (Art.. 35 DS-GVO) in besonders geeignet, diesen Nachweis zu erbringen.

Die folgenden, auf den spezifischen Schutzbedarf von Betroffenen ausgerichteten Datenschutz-Gewährleistungsziele geben die datenschutzrechtlichen Anforderungen in einer praktisch umsetzbaren Form wieder:

4. Nichtverkettung,
5. Transparenz und
6. Intervenierbarkeit.

(4) Das Gewährleistungsziel Nichtverkettung bezeichnet die Anforderung, dass Daten nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben werden.

Datenbestände sind prinzipiell dazu geeignet, für weitere Zwecke eingesetzt zu werden und mit anderen, unter Umständen öffentlich zugänglichen Daten kombiniert zu werden. Je größer und aussagekräftiger Datenbestände sind, umso größer sind erfahrungsgemäß die Begehrlichkeiten, die Daten zweckentfremdet, über die Rechtsgrundlage hinaus, zu nutzen.

Rechtlich zulässig sind derartige Weiterverarbeitungen jedoch nur unter eng definierten Umständen. Die DS-GVO lässt sie nur zu für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke und fordert für diese Fälle ausdrücklich Garantien für die Rechte und Freiheiten der betroffenen Personen. Diese Garantien sollen durch technische und organisatorische Maßnahmen sichergestellt werden. Neben Maßnahmen zur Datenminimierung und zur Pseudonymisierung sind hierfür auch Maßnahmen geeignet, mit denen die Weiterverarbeitung organisations- bzw. systemseitig getrennt von der Ursprungsverarbeitung geschieht. Der Datenbestand kann bspw. durch Pseudonymisierung und Reduzierung auf den für den neuen Zweck erforderlichen Umfang angepasst werden.

(5) Das Gewährleistungsziel *Transparenz* bezeichnet die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt. Transparenz ist für die Beobachtung und Steuerung von Daten, Prozessen und Systemen von ihrer Entstehung bis zu ihrer Löschung erforderlich und eine Voraussetzung dafür, dass eine Datenverarbeitung rechtskonform betrieben und in diese, soweit erforderlich, von Betroffenen informiert eingewilligt werden kann. Transparenz der gesamten Datenverarbeitung und der beteiligten Instanzen kann dazu beitragen, dass insbesondere Betroffene und Kontrollinstanzen Mängel erkennen und ggf. entsprechende Verfahrensänderungen einfordern können.

(6) Das Gewährleistungsziel *Intervenierbarkeit* bezeichnet die Anforderung, dass den Betroffenen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen. Dazu müssen die für die Verarbeitungsprozesse verantwortlichen Stellen jederzeit in der Lage sein, in die Datenverarbeitung vom Erheben bis zum Löschen der Daten einzugreifen.

5.5 Weitere abgeleitete Gewährleistungsziele

Einige Landesdatenschutzgesetze verwenden Gewährleistungsziele, die sich nicht mit den Gewährleistungszielen des SDM decken. Sie lassen sich jedoch aus den oben genannten elementaren Gewährleistungszielen ableiten. Folgende abgeleitete Gewährleistungsziele sind insbesondere zu nennen:

Das Gewährleistungsziel der *Authentizität* beschreibt die Anforderung, dass personenbezogene Daten ihrem Ursprung gesichert zugeordnet werden können.

Je nach Art des Ursprungs sind unterschiedliche Angaben festzuhalten und die Verknüpfung der Daten mit diesen Angaben zu schützen: Im Falle von Erhebungen bei den Betroffenen selbst schließen diese Angaben den Erhebungsprozess, den Zeitpunkt seines Ablaufs und ggf.

die Identität der erhebenden Personen ein; im Falle der Entgegennahme von Übermittlungen oder dem Abruf aus Datenbeständen Dritter sind dies Zeitpunkt, Anlass und Zweck von Übermittlung bzw. Abruf, sowie die Datenquelle; im Falle einer Zweck ändernden Übernahme eines Datenbestandes Bezeichnung und Revisionsstand des Quelldatenbestandes sowie ein Verweis auf dessen Dokumentation.

Dieses Gewährleistungsziel ist in das umfassendere Ziel der Wahrung der Transparenz der Verarbeitung einzuordnen. Es ist nur unter Wahrung der Integrität der Verknüpfung zwischen Datenbestand und Ursprung zu erreichen, so dass es auch als eine Form der „integritätsgesicherten Transparenz“ aufgefasst werden kann.

Das Gewährleistungsziel der *Revisionsfähigkeit* beschreibt die Anforderung, dass festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Es nimmt sowohl ändernde Verarbeitungen als auch Nutzungen und bloße Kenntnisnahmen in Betracht. Auch dieses Gewährleistungsziel ist in das umfassendere Ziel der Gewährleistung der Transparenz der Verarbeitung einzuordnen und nur unter Wahrung der Integrität der Verknüpfung zwischen Datenbestand und Verarbeitungsnachweis zu erreichen.

6 Der Bezug der Gewährleistungsziele zum bestehenden Datenschutzrecht

Normen lassen sich nicht ohne weiteres technisch operationalisieren. In der datenschutzrechtlichen Prüfung müssen Juristen und Informatiker deshalb eine gemeinsame Sprache finden, um sicherzugehen, dass die rechtlichen Anforderungen auch tatsächlich technisch umgesetzt werden. Hierbei werden sie durch die Gewährleistungsziele unterstützt, denn die datenschutzrechtlichen Anforderungen können entsprechend ihres Gehalts, ihrer beabsichtigten Wirkung und Zielrichtung den einzelnen Gewährleistungszielen zugeordnet und auf diese Weise strukturiert gebündelt werden. Die technische Gestaltung von Systemen kann sich an diesen auf Umsetzbarkeit hin ausgerichteten Zielen orientieren, so dass die datenschutzrechtlichen Anforderungen über die Gewährleistungsziele in erforderliche technische und organisatorische Maßnahmen transformiert werden können.

6.1 Gewährleistungsziele in der Rechtsprechung des Bundesverfassungsgerichts

Die Gewährleistungsziele beinhalten ausschließlich Forderungen, die gesetzlich gedeckt sind. Sie entsprechen letztlich den Grundprinzipien zur Absicherung des Rechts auf informationelle Selbstbestimmung (vgl. Ziffer 5.2), wie sie sich aus dem Volkszählungsurteil (BVerfG, Urteil vom 15.12.1983, 1 BvR 209/83 u. a.) ergeben. Das BVerfG hatte dort darauf hingewiesen, dass die freie Entfaltung der Persönlichkeit unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraussetzt. Vor dem Hintergrund der der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten hatte das BVerfG auf den Schutz des Betroffenen gegen Zweckentfremdung der Datenverarbeitung Bezug genommen. Im Schwerpunkt befasst sich die Entscheidung mit der Transparenz für die Betroffenen und deren Selbstbestimmung, d. h. die Betroffenen sollen überschauen können, welche Informationen über sie bekannt sind, um dann aus eigener Selbstbestimmung planen und entscheiden zu können.

Darüber hinaus hat das BVerfG festgelegt, dass der Gesetzgeber organisatorische und verfahrensrechtliche Vorkehrungen zu treffen hat, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken. So gelten nach den Ausführungen im Urteil z. B. Weitergabe- und Verwertungsverbote sowie Aufklärungs-, Auskunfts- und Löschungspflichten als wesentliche verfahrensrechtliche Schutzvorkehrungen. Aus der Rechtsprechung des BVerfG sind daher die Grundideen der Zweckbindung/Nichtverkettung, Erforderlichkeit, Transparenz und Intervenierbarkeit sowie der Sicherheit der Datenverarbeitung ableitbar, die flankiert durch die daran ausgerichtete Verfahrensgestaltungen, das Recht auf informationelle Selbstbestimmung schützen bzw. zu dessen Entfaltung beitragen sollen.

In der Entscheidung zum heimlichen Zugriff auf informationstechnische Systeme (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07 u. a.) hat das BVerfG das Grundrecht auf Gewähr-

leistung der Integrität und Vertraulichkeit informationstechnischer Systeme entwickelt. Unter bestimmten Umständen unterliegen damit auch informationstechnische Systeme insgesamt einer eigenständigen, persönlichkeitsrechtlichen Gewährleistung von Vertraulichkeit und Integrität und nicht nur einzelne Kommunikationsvorgänge oder gespeicherte Daten. Der Schutzbereich des Grundrechts ist nach den Feststellungen des BVerfG allerdings nur dann eröffnet, wenn

- die Betroffenen zur Persönlichkeitsentfaltung auf die Nutzung des Systems angewiesen sind
- das System personenbezogene Daten des Betroffenen in einem Umfang und einer Vielfalt enthalten kann, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten
- und wenn der Betroffene das System als eigenes nutzt und dementsprechend davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt.

In diesen Fällen darf der Betroffene erwarten, dass seine von dem informationstechnischen System erzeugten, verarbeiteten oder gespeicherten Daten vertraulich bleiben und nicht so auf das System zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch (nicht verfügungsbefugte) Dritte genutzt werden können, womit die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen wäre. Jedenfalls in Fällen, in denen informationstechnische Systeme von den Betroffenen als eigene Systeme genutzt aber von Dritten betrieben werden, kann das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit von informationstechnischen Systemen als direkte verfassungsrechtliche Verankerung der Gewährleistungsziele Vertraulichkeit und Integrität angesehen werden. Über die mittelbare Drittwirkung der Grundrechte kann sich dies auch im Verhältnis Privater zueinander auswirken, so z. B. im Falle von Cloud Services für Private, die mehr und mehr eine zentrale Back-up-Funktion für sämtliche digitalisierte persönliche Informationen erfüllen oder solche Informationen erzeugen. Darüber hinaus können Mobiltelefone bzw. Smartphones informationstechnische Systeme darstellen, deren Absicherung gewährleistet sein muss, auch im Zuge der Nutzung von Dienstleistungen, bei denen diese Geräte mit der IT öffentlicher und privater Stellen interagieren. Soweit die Nutzung des eigenen informationstechnischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden, erstreckt sich der Schutz des Nutzers auch hierauf.

6.2 Verankerung der Gewährleistungsziele im BDSG

6.2.1 Gewährleistungsziele als Prüfungsmaßstab

Ausgangspunkt ist § 9 S. 1 BDSG. Dort heißt es:

„Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten."

§ 9 Satz 1 BDSG legt fest, dass die datenschutzrechtlichen Anforderungen durch die Umsetzung von technischen und organisatorische Maßnahmen zu gewährleisten sind. Die rechtliche Abwägung darüber, ob „der mit diesen Maßnahmen verbundene Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht", muss bereits bei der Planung der Maßnahmen etwa im Zusammenhang mit einer Schutzbedarfsfeststellung stattgefunden haben und entschieden sein. Zur Ermittlung, welche Maßnahmen zur Einhaltung der Gesetze geeignet und erforderlich und somit angemessen sein können, dienen die Gewährleistungsziele, die auf der einen Seite die datenschutzrechtlichen Anforderungen bündeln und strukturieren und auf der anderen Seite durch technische Umsetzung erreicht werden können.

Die verantwortliche Stelle ist verpflichtet, die entsprechenden technischen und organisatorischen Maßnahmen vorab festzulegen und dies auch entsprechend nachweisen zu können. Das BVerfG hatte im Volkszählungsurteil (BVerfG, Urteil vom 15.12.1983, 1 BvR 209/83) von dem Gesetzgeber verlangt, dass dieser organisatorische und verfahrensrechtliche Vorkehrungen zu treffen hat, welche bereits der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken. Dementsprechend ist § 9 Satz 1 BDSG sowie Satz 1 der Anlage zu § 9 BDSG formuliert: Nur wer vorab die innerbehördliche oder innerbetriebliche Organisation so gestaltet hat, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird, und die erforderlichen und angemessenen Maßnahmen getroffen hat, kann für alle folgenden Ereignisse die Gewähr übernehmen, dass die Vorschriften eingehalten werden. Sofern danach die Pflicht besteht, die Maßnahmen vorab festzulegen (etwa in einem vorab zu erstellenden Sicherheitskonzept), muss die Erfüllung dieser Pflicht – insbesondere nach den Vorgaben der DS-GVO – nachgewiesen werden können. Auch die Datenschutz-Richtlinie 95/46/EG macht in Erwägungsgrund 46 deutlich, dass bereits zum Zeitpunkt der Planung des Verarbeitungssystems geeignete technisch-organisatorische Maßnahmen getroffen werden sollen, um insbesondere die Sicherheit der Verarbeitung zu gewährleisten und jede unrechtmäßige Verarbeitung zu verhindern. Das Verbot mit Erlaubnisvorbehalt in § 4 Abs. 1 BDSG zwingt die verantwortliche Stelle dazu, vor der Datenverarbeitung zu wissen, ob diese zulässig ist oder nicht. Zu diesem Zeitpunkt muss sie folglich bereits nachweisen können, dass die Einhaltung der Vorschriften auch durch technische und organisatorische Maßnahmen gewährleistet ist.

Die datenschutzrechtlichen Vorschriften können, ihrem Gehalt und ihrer Zielrichtung entsprechend, den Gewährleistungszielen zugeordnet werden (sog. „Mapping"). Diese Strukturierung ermöglicht die Operationalisierung der datenschutzrechtlichen Anforderungen in prüffähiger und standardisierter Form, so wie es im Bereich des BSI-Grundschutzes seit Mitte der 90er Jahre bewährte Praxis ist. Auf diese Weise wird die verantwortliche Stelle darüber

hinaus unterstützt, den Nachweis darüber zu führen, dass die erforderlichen Maßnahmen zur Vermeidung von Rechtsverstößen auch tatsächlich ergriffen wurden.

Wie das Mapping erfolgen kann, sollen die nachfolgenden Beispiele sowie die „Mapping-Tabelle“ verdeutlichen.

Datenminimierung

In § 3a BDSG ist (abweichend vom Begriff der Datenminimierung in der DS-GVO) das Gebot der Datensparsamkeit geregelt, das sich aus dem allgemeinen Grundsatz der Erforderlichkeit ergibt, der als zentrale Voraussetzung in den Erlaubnistatbeständen zum Ausdruck kommt (z. B. § 28 BDSG). Die Regelung des § 3a Satz 1 BDSG stellt klar, dass der Grundsatz insbesondere bei der Auswahl und Gestaltung von Datenverarbeitungssystemen anzuwenden ist.

Spezielle Anforderungen ergeben sich z. B. aus der Löschpflicht bei weggefallener Erforderlichkeit (§ 20 Abs. 2 Nr. 2 und § 35 BDSG), oder der Anonymisierungspflicht in § 30 a Abs. 3 BDSG.

Verfügbarkeit

Dieses Gewährleistungsziel ist in der Nr. 7 der Anlage zu § 9 BDSG niedergelegt. Die Anforderung den Verlust der Daten zu vermeiden, beinhaltet auch die Nutzbarkeit der Daten (und eine Auskunftsfähigkeit über sie) zu gewährleisten, da ein Verlust dieser Fähigkeit einem Verlust der Daten in der Auswirkung für den Verarbeitungszweck gleich kommt.

Auch Art. 17 Abs. 1 Satz 1 Datenschutz-Richtlinie 95/46/EG fordert geeignete Maßnahmen für einen Schutz gegen die zufällige oder unrechtmäßige Zerstörung oder den zufälligen Verlust personenbezogener Daten.

Integrität

Aus den Anforderungen von Nr. 3 und Nr. 4 der Anlage zu § 9 BDSG, unbefugte Veränderungen und Entfernungen auszuschließen, ist das Gewährleistungsziel Integrität auf der Ebene der Daten abzuleiten. Die Anforderung der Gewährleistung der Integrität auf der Systemebene folgt aus dem allgemeinen Grundsatz der Gewährleistung einer rechtskonformen Datenverarbeitung (§ 9 BDSG).

Auch Art. 17 Abs. 1 Datenschutz-Richtlinie 95/46/EG fordert geeignete Maßnahmen für einen Schutz gegen eine unberechtigte Änderung personenbezogener Daten. Weiterhin besteht seit der Entscheidung des Bundesverfassungsgerichts vom 27.2.2008 (BVerfG, 1 BvR 370/07) ein „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ (s. o.) zumindest für den Bereich der Datenverarbeitung im öffentlichen Bereich.

Vertraulichkeit

Die Verpflichtung zur Wahrung der Vertraulichkeit ergibt sich insbesondere aus den Gewährleistungspflichten der Nr. 3 und Nr. 4 der Anlage zu § 9 BDSG, aus Art. 16 sowie Art. 17 Abs. 1 der Datenschutz-Richtlinie 95/46/EG und aus § 5 BDSG (Datengeheimnis).

Nichtverkettung

Die Verpflichtung, Daten *nur für den Zweck* zu verarbeiten, zu dem sie erhoben wurden, ist insbesondere den einzelnen Verarbeitungsbefugnissen zu entnehmen, die die Geschäftszwecke, die Forschungszwecke etc. zum Maßstab machen. Bei der Datenverarbeitung auf der Grundlage der Einwilligung ergibt sich aus § 4a Abs. 1 Satz 2 BDSG, dass auf den vorgesehenen Zweck hinzuweisen ist. Der Zweck ist demnach festzulegen und die Einwilligung erstreckt sich nur auf die Verarbeitung zu diesem Zweck.

Auch Art. 6 Abs. 1 b) und c) der Datenschutz-Richtlinie 95/46/EG sehen die zweckgebundene Datenverarbeitung vor.

Die Verpflichtung zur Festlegung der Zwecke ergibt sich zudem aus den Vorgaben zur Erstellung eines Verfahrensverzeichnisses bzw. zur Meldung automatisierter Verfahren (§§ 4d Abs. 1, 4g Abs. 2 Satz 1, 4 e) sowie aus § 28 Abs. 1 Satz 2 BDSG.

Die spezifische Forderung nach Datentrennung ist in Nr. 8 der Anlage zu § 9 BDSG niedergelegt.

Transparenz

Für die Betroffenen sind sowohl in der Datenschutz-Richtlinie 95/46/EG (Art. 10, 11, 12) als auch im BDSG (§§ 4 Abs. 3, 4a Abs. 1 Satz 2, 33, 34 BDSG) Informations-, Benachrichtigungs- und Auskunftsrechte geregelt. Die verantwortlichen Stellen müssen, gem. Satz 1 der Anlage zu § 9 BDSG, die Voraussetzung für die Gewährung dieser Rechte sowohl auf organisatorischer, als auch, soweit erforderlich, auf technischer Ebene schaffen.

Für die *verantwortliche Stelle* ergibt sich zunächst aus § 4 Abs. 1 BDSG die Pflicht, personenbezogene Daten nur auf der Grundlage einer Rechtsvorschrift oder Einwilligung zu verarbeiten. Da die Vorschrift als Verbot mit Erlaubnisvorbehalt formuliert ist, muss die verantwortliche Stelle letztlich geprüft haben, ob eine Befugnis zur Verarbeitung besteht. Daraus ergibt sich grundsätzlich, dass die verantwortliche Stelle sämtliche Verarbeitungen personenbezogener Daten in ihrem Verantwortungsbereich kennen muss, um diese bewerten zu können. Spezifische Anforderungen zur Herstellung interner Transparenz ergeben sich aus den §§ 4d Abs. 1, 4e sowie §§ 4g Abs. 2, 4e BDSG.

Zudem sind Verfahrensverzeichnisse (als notwendiger Teil einer umfassenden Gesamtdokumentation eines Verfahrens) zu erstellen, die, mit Ausnahme des Aspekts der technisch-organisatorischen Maßnahmen, von *jedermann* gemäß § 38 Abs. 2 BDSG bzw. § 4g Absatz 2 Satz 2 BDSG eingesehen werden können.

Intervenierbarkeit

Die Interventionsrechte der Betroffenen ergeben sich explizit aus den Vorschriften zu Berichtigung, Sperrung, Löschung und Widerspruch. Sie können sich außerdem als Ergebnis einer Interessenabwägung im Rahmen eines gesetzlichen Erlaubnistatbestandes ergeben. Wiede-

rum müssen die verantwortlichen Stellen gem. Satz 1 der Anlage zu § 9 BDSG die Voraussetzung für die Gewährung dieser Rechte, sowohl auf organisatorischer als auch, soweit erforderlich, auf technischer Ebene schaffen.

Tabelle 1: Zuordnung der gesetzlichen Vorgaben des BDSG zu den Gewährleistungszielen.

	Datemini-mierung	*Verfügbar-keit*	*Integrität*	*Vertraulich-keit*	*Nichtver-kettung*	*Transpa-renz*	*Intervenier-barkeit*
§ 3a	§ 3a						
§ 4	§ 4 Abs. 2 Nr. 2a				§ 4 Abs. 3 Nr. 2	§ 4 Abs. 3	§ 4 Abs. 1
§§ 4a, 4b, 4c, 4d, 4e, 4f, 4g					§ 4a Abs. 1 Satz 2 § 4b Abs. 6 § 4c Abs. 1 Satz 2 § 4e Nr. 4	§ 4a Abs. 1 Satz 2-4, Abs. 2Satz 2, Abs. 3 § 4d Abs. 1 Satz 1, § 4d Abs. 5 § 4e § 4g Abs. 2	§ 4c Abs. 1 Satz 1 Nr. 1
§ 5				§ 5 Satz 1, Satz 2, Satz 3			
§§ 6, 6a, 6b, 6c	§ 6b Abs. 1, Abs. 3, Abs. 5				§ 6 Abs. 3 § 6b Abs. 1, § 6b Abs. 3 Satz 3, § 6b Abs. 5	§ 6 Abs. 1, Abs. 2 Sätze 1-3 § 6a Abs. 2 Nr. 2 § 6b Abs. 2, Abs. 3,§ 6b Abs. 4 § 6c Abs. 1, Abs. 3	§ 6 Abs. 1, § 6 Abs. 2 Satz 1 § 6a Abs. 1 Satz 1, Abs. 2 Nr. 2
§ 9	§ 9 Satz 1	§ 9 Satz 1 Nr. 7 Anlage zu § 9	§ 9 Satz 1 Nr. 3, Nr. 4, Nr. 5 Anlage zu § 9	§ 9 Satz 1 Nr. 3, Nr. 4 Anlage zu § 9	§ 9 Satz 1 Nr. 8 Anlage zu § 9	§ 9 Satz 1 Nr. 1-6 Anlage zu § 9	§ 9 Satz 1
§ 10					§ 10 Abs. 2 Nr. 1	§ 10 Abs. 2, Abs. 3, Abs. 4 Satz 3	
§ 11	§ 11 Abs. 2 Satz 2 Nr. 10	§ 11 Abs. 2 Satz 2 Nr. 3	§ 11 Abs. 2 Satz 2 Nr. 3	§ 11 Abs. 2 Satz 2 Nr. 3 § 11 Abs. 2 Satz 2 Nr. 10	§ 11 Abs. 2 Satz 2 Nr. 2 § 11 Abs. 2 Satz 2 Nr. 10	§ 11 Abs. 2	§ 11 Abs. 2 Satz 2 Nr. 4

	Datemini-mierung	*Verfügbar-keit*	*Integrität*	*Vertraulich-keit*	*Nichtver-kettung*	*Transpa-renz*	*Intervenier-barkeit*
§ 28, 28a	§ 28 Abs. 1 Satz 1 Nr. 1, Nr. 2, Abs. 2, Abs. 3 Satz 2, Abs. 6-9 § 28 a Abs. 1	§ 28 Abs. 3a Satz 1	§ 28 Abs. 3a Satz 1		§ 28 Abs. 1 Satz 1 Nr. 1, Nr. 2, Abs. 1 Satz 2, Abs. 2, § 28 Abs. 3 Satz 1, Satz 2, Satz 3, Satz 4, Satz 5, Satz 7, Abs. 5, Abs. 6-9 § 28a Abs. 1, Abs. 2, § 28a Abs. 2 Satz 4	§ 28 Abs. 3 Satz 4, Satz 5, § 28a Abs. 3 § 28a Abs. 2 Satz 2, Abs. 3	§ 28 Abs. 3a Satz 1, Abs. 4
§ 29					§ 29 Abs. 1, Abs. 2, Abs. 4	§ 29 Abs. 2 Satz 2, Satz 3, Satz 4, Abs. 7 Satz 1	§ 29 Abs. 3, Abs. 4
§ 30	§ 30 Abs. 1 § 30 a Abs. 3						
§ 31					§ 31		
§§ 33-35	§ 35					§§ 33, 34	§§ 33-35
§ 38						§ 38 Abs. 1 Satz 5	
§ 39					§ 39		
§ 40	§ 40				§ 40		
§ 42a						§ 42a	

6.2.2 Verankerung der Anwendbarkeit der Gewährleistungsziele auf personenbezogene Verfahren

Zwar knüpfen die materiellrechtlichen Vorgaben zumeist erst an konkrete Datenverarbeitungen an, die Pflicht der verantwortlichen Stelle, Rechtsverstöße zu verhindern, führt aber wie gezeigt dazu, dass technisch-organisatorische Maßnahmen bereits bei der Verfahrensgestaltung berücksichtigt werden müssen, damit diese bei der Datenverarbeitung in Produktion auch berücksichtigt werden können. Die Operationalisierung der datenschutzrechtlichen Anforderungen erfordert daher, dass personenbezogene Verfahren in den Blick zu nehmen sind, so dass die durch die Maßnahmen zu erreichenden Gewährleistungsziele auch beim Verfahren ansetzen müssen.

Das BDSG enthält eine Reihe von Vorschriften, die das Verfahren als solches in den Blick nehmen und hierfür Anforderungen formulieren (vgl. §§ 4d Abs. 1, 4d Abs. 5, 6c Abs. 1, § 10 Abs.

1, § 28b Nr. 1, § 29 Abs. 2 S. 3, § 38 Abs. 5 S. 2, § 43 Abs. 2 Nr. 2 BDSG). Dabei werden zum Teil gesetzliche Anforderungen an Verarbeitungen bzw. Verfahren gestellt, die (noch) keinen Personenbezug aufweisen oder bei welchen ein solcher nicht ausgeschlossen werden kann (§§ 11 Abs. 5, b Nr. 1, § 34 Abs. 2, 3, 4; außerdem z. B. § 13 Abs. 1 S. 2 TMG). Ausdrücklich wird auf Verfahren im Rahmen der Meldepflichten und Vorabkontrollen abgestellt (§ 4e BDSG).

Danach sieht das Gesetz selbst im Hinblick auf die Verankerung von Anforderungen keine strikte Trennung zwischen konkreten Datenverarbeitungen und Verfahrensvorgaben vor.

6.3 Verankerung der Gewährleistungsziele in den Landesdatenschutzgesetzen

Hier sind zunächst zwei Kategorien zu bilden. Etliche Landesdatenschutzgesetze sehen wie das BDSG bestimmte Kontrollen vor (Bremen, Hessen, Rheinland-Pfalz, Saarland, Bayern, Baden-Württemberg und Niedersachsen). Für diese Länder ist auf die Ausführungen zum BDSG (oben 6.2) zu verweisen.

Eine ganze Reihe von Datenschutzgesetzen enthalten jedoch Anforderungen, die als „Schutzziele“ formuliert sind und somit bereits einige Gewährleistungsziele abbilden. Die Datenschutzgesetze der neuen Bundesländer sowie die Datenschutzgesetze von Berlin, Hamburg und Nordrhein-Westfalen enthalten die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit, sowie Transparenz (ohne Hamburg), Authentizität und Revisionsfähigkeit. Das Landesdatenschutzgesetz von Schleswig-Holstein enthält seit Januar 2012 den vollständigen Satz der oben aufgeführten Gewährleistungsziele, wobei dort noch der Begriff der Nichtverkettbarkeit verwendet wird.

Ausgangspunkt sind die jeweiligen Vorschriften zu technischen und organisatorischen Maßnahmen. Diese fordern, eine gesetzeskonforme Datenverarbeitung zu gewährleisten. Keinen wesentlichen Unterschied macht es dabei, ob die Schutzziele beispielhaft (Mecklenburg-Vorpommern: „insbesondere“) oder abschließend formuliert sind. In jedem Fall können sich Gewährleistungsziele nicht nur aus den Schutzzielen, sondern auch aus materiellrechtlichen Vorgaben ergeben.

Dabei ist jedoch zu beachten, dass sich die gesetzlich vorgegebene Ausprägung des Schutzziels Transparenz von dem gleichlautenden Gewährleistungsziel des SDM unterscheidet. Während erstere lediglich die Dokumentation der Verfahrensweisen beinhaltet, umfasst letztere auch die Authentizität oder Revisionsfähigkeit konkreter Datenverarbeitungen sowie Informations-, Benachrichtigungs- und Auskunftsrechte. Damit sind nur die Gewährleistungsziele „Nichtverkettung“, „Intervenierbarkeit“ und „Datenminimierung“ nicht bereits in bestehenden Schutzzielen verankert. Hierzu kann jedoch auf die oben gemachten Ausführungen im Rahmen des BDSG verwiesen werden.

In der nachfolgenden Mapping-Tabelle wird beispielhaft das Sächsische Datenschutzgesetz daraufhin untersucht, wie die dort vorhanden Vorschriften auf die Gewährleistungsziele des SDM abgebildet werden können.

Tabelle 2: Zuordnung der gesetzlichen Vorgaben des SächsDSG zu den Gewährleistungszielen

Daten-minimierung	*Verfügbarkeit*	*Integrität*	*Vertraulichkeit*	*Nichtverkettung*	*Transparenz*	*Intervenierbarkeit*
§ 9 Abs. 1 Satz 2	§ 9 Abs. 2 Nr. 3	§ 9 Abs. 2 Nr. 2	§ 9 Abs. 2 Nr. 1		§ 9 Abs. 2 Nrn. 4-6	
§§ 20, 21 Abs. 2 Satz 2 (Löschung/ Sperrung bei entfallener Erforderlichkeit)				§ 4 Abs. 3 (Zweckfestlegung bei Einwilligung)	§ 4 Abs. 3 (informierte Einwilligung)	§ 4 Abs. 1 Nr. 2 (Einwilligung/ Rücknahme)
§ 36 Abs. 2 (Pseudonym./ Anonym. bei wiss. Forschung)				§ 10 Abs. 1 Nr. 2 (Zweckbestimmung im Verfahrensverzeichnis)	§ 5 (Betroffenenrechte)	§§ 19-21 (Berichtigung, Löschung, Sperrung)
§ 33 Abs. 4 (Löschfrist bei Videoaufzeichnungen)				§ 12 Abs. 2, 5, 6 (Zweckfest-legung bei Erhebung)	§3 10, 11 Abs. 4 Nr. 5, 31 Abs. 2 (Verfahrensverzeichnis)	§ 32 Abs. 1 (Fernmessen und Fernwirken)
§ 12 (Erhebung nur bei Erforderlichkeit)				§ 13 (Zweckbindung bei Speicherung etc.)	§ 12 (Datenerhebung)	
§ 13 (Speicherung etc. nur bei Erforderlichkeit)				§§ 14 Abs. 3, 16 Abs. 4 (Zweckbindung bei Übermittlung)	§§ 18, 34 Abs. 3 (Auskunft)	
§§ 14, 15, 16, 17 (Übermittlung nur bei Erforderlichkeit)				§ 32 Abs. 1 (Zweckbindung bei Fernmessen und Fernwirken)	§ 27 (Kontrolle)	
				§ 33 (Zweckbindung Video)	§ 32 (Fernmessen und Fernwirken)	
				§ 34 (automatisierte Einzelentscheidung)	§ 33 Abs. 3 (Videoüberwachung)	

6.4 Verankerung der Gewährleistungsziele in der EU-Datenschutz-Grundverordnung

Mit der EU-Datenschutz-Grundverordnung (DS-GVO) wird das Datenschutzrecht europaweit einheitlich geregelt. Die Verordnung, die am 25.05.2016 in Kraft getreten ist wird gem. Art. 99 Abs. 2 DS-GVO ab dem 25.05.2018 unmittelbar in allen EU Mitgliedstaaten gelten. Den nationalen Gesetzgebern wurden durch zahlreiche Öffnungsklauseln ergänzende Regelungsbefugnisse geschaffen. Jedoch besteht für die DS-GVO ein grundsätzlicher Anwendungsvorrang vor nationalem Recht. Die Gewährleistungsziele finden ihren ganz wesentlichen Anker in den Grundsätzen der Verarbeitung personenbezogener Daten in Art. 5 DS-GVO, die wiederum den Schutzauftrag aus Art. 8 der Charta der Grundrechte der Europäischen Union aufnehmen.

Entsprechend verpflichtet die DS-GVO die verantwortlichen Stellen und verarbeitenden Organisationen dazu, zur Gewährleistung des grundrechtlichen Schutzes der Rechte der Betroffenen sowie gegen unbefugte Zugriffe durch Dritte die dafür angemessenen technischen und organisatorischen Maßnahmen (insbes. Art.. 32 DS-GVO) auszuwählen und im Rahmen der Technikgestaltung und datenschutzfreundlicher Voreinstellungen gem. Art. 25 DS-GVO einzusetzen und zu prüfen (Art.. 32 I d). Der Verantwortliche ist für die Einhaltung der Grundsätze der Verarbeitung nach Art. 5 Abs. 1, 24 DS-GVO verantwortlich und muss dessen Einhaltung nachweisen können. Des Weiteren verlangt die DS-GVO für Verarbeitungen mit möglicherweise hohem Risiko für die Rechte und Freiheiten natürlicher Personen einer Datenschutz-Folgenabschätzung (Art. 35 DS-GVO, DPIA). Sie basiert auf einer systematischen Beschreibung der geplanten Verarbeitungsvorgänge und fordert im Ergebnis Maß-nahmen zur Bewältigung der erwarteten Risiken. Dies schließt Garantien, Sicherheitsvorkehrungen und Verfahren ein, durch die der Schutz personenbezogener Daten sichergestellt, nachgewiesen und überprüft werden kann (Art. 35 Abs. 7, 11 DS-GVO). Das SDM soll Organisationen dabei unterstützen, den Übergang zur DS-GVO transparent, kontrolliert und ressourcenschonend zu vollziehen. Es soll dazu beitragen, die in Art. 5 formulierten Grundsätze für die Verarbeitung personenbezogener Daten umzusetzen und mit überschaubarem Aufwand die von der DS-GVO geforderten Umsetzungsnachweise (bspw. gem. Art. 5 Abs. 2, Art. 24 Abs.1) zu erbringen.

Auch im Zusammenhang mit der Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen kann das SDM ein geeignetes Hilfsmittel sein. Mit Hilfe des SDM können auch für diese Fälle technische und organisatorische Maßnahmen abgeleitet werden, die in den Text für geeignete Garantien gem. Art. 46 DS-GVO oder für verbindliche interne Datenschutzvorschriften (Binding Corporate Rules - BCR) gem. Art. 47 DS-GVO eingehen. Das SDM unterstützt beispielsweise bei der Auswahl von geeigneten und angemessenen Maßnahmen für Verfahren insbesondere bzgl. der Dokumentation und Protokollierung, die in vielen Ländern seit Jahren als Stand der Technik von Datenschutzaufsichtsbehörden gefordert werden.

Die Gewährleistungsziele Integrität, Verfügbarkeit, Vertraulichkeit, Transparenz und Datenminimierung finden sich unmittelbar begrifflich im Verordnungstext wieder, wobei auch Bezug auf Anforderungen der IT-Sicherheit genommen wird. Die Gewährleistungsziele Nichtverkettung und Intervenierbarkeit sind als Schutzziele in zahlreichen Einzelnormen u.a. über den Zweckbindungsgrundsatz, die Löschung und Datenportabilität aufgenommen worden.

Die folgenden Ausführungen und Tabellen verschaffen einen Überblick über die Zuordnung der Gewährleistungsziele zu den Artikeln und den Erwägungsgründen der DS-GVO.

Verfügbarkeit

Der Grundsatz der Verfügbarkeit ist in Art. 32 Abs. 1 b) und c) explizit im Kontext der Sicherheit von Datenverarbeitungen aufgenommen. Es ist zudem in Art. 5 Abs. 1 e) DS-GVO als Voraussetzung für die Identifizierung der betroffenen Person verankert. Es gewährleistet die Verfügbarkeit der Daten zu dem jeweiligen Zweck, solange dieser noch besteht. Der Grundsatz kommt zum Tragen bei den Informations- und Auskunftspflichten (Art. 13 und 15 DS-GVO) gegenüber den Betroffenen. Für das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO) ist das Gewährleistungsziel der Verfügbarkeit ebenso Grundvoraussetzung.

Integrität

Das Gewährleistungsziel der Integrität ist in Art. 5 Abs. 1 f) DS-GVO als Grundsatz für die Verarbeitung von Daten und in Art. 32 Abs. 1 b) DS-GVO als Voraussetzung für die Sicherheit einer Datenverarbeitung genannt. Es soll unbefugte Veränderungen und Entfernungen auszuschließen.

Vertraulichkeit

Die Verpflichtung zur Wahrung der Vertraulichkeit ergibt sich insbesondere aus Art. 5 Abs. 1 f) DS-GVO, aus Art. 32 Abs. 1 b) DS-GVO sowie Art. 38 Abs. 5 DS-GVO (Geheimhaltungspflicht des Datenschutzbeauftragten) bzw. Art. 28 Abs. 3 b) DS-GVO (Geheimhaltungspflicht des Auftragsdatenverarbeiters). Es gewährleistet den Schutz vor unbefugter und unrechtmäßiger Verarbeitung. Eine Verletzung der Vertraulichkeit stellt in der Regel eine Datenverarbeitung ohne Rechtsgrundlage dar.

Nichtverkettung

Die Verpflichtung, Daten nur für den Zweck zu verarbeiten, zu dem sie erhoben wurden, ist insbesondere den einzelnen Verarbeitungsbefugnissen zu entnehmen, die die Geschäftszwecke, die Forschungszwecke etc. zum Maßstab machen und findet über den Zweckbindungsgrundsatz aus Art. 5 Abs. 1 c) DS-GVO Eingang in die Grundverordnung. Bei der Datenverarbeitung auf der Grundlage der Einwilligung ergibt sich aus Art. 7 Abs. 4 DS-GVO, dass eine Einwilligung unwirksam sein kann, wenn die Daten zu Zweckerfüllung nicht erforderlich sind.

Eine typische Maßnahme der Nichtverkettung ist etwa die Pseudonymisierung und wird beispielsweise in Art. 40 Abs. 2 d) DS-GVO genannt.

Transparenz

Der Grundsatz der Transparenz ist in Art. 5 Abs. 1 a) DS-GVO festgeschrieben. Er findet sich als tragender Grundsatz des Datenschutzrechts in zahlreichen Regelungen der DS-GVO. Insbesondere die Informations- und Auskunftspflichten tragen ihm Rechnung.

Intervenierbarkeit

Die Interventionsrechte der Betroffenen ergeben sich explizit aus den Vorschriften zu Berichtigung, Sperrung, Löschung und zum Widerspruch (Art. 16. 17 DS-GVO). Sie können sich außerdem als Ergebnis einer Interessenabwägung im Rahmen eines gesetzlichen Erlaubnistatbestandes ergeben. Wiederum müssen die verantwortlichen Stellen gem. Art. 5 Abs. 1 d) DS-GVO die Voraussetzung für die Gewährung dieser Rechte, sowohl auf organisatorischer als auch, soweit erforderlich, auf technischer Ebene schaffen.

Tabelle 3: Zuordnung der Artikel der DS-GVO zu den Gewährleistungszielen.

Datenminimierung	*Verfügbarkeit*	*Integrität*	*Vertraulichkeit*	*Nichtverkettung*	*Transparenz*	*Intervenierbarkeit*
5 I c), 5 I e), 25, 32	5 I e), 13, 15, 20, 25, 32	5 I f), 25, 32, 33	5 I f), 25, 28 III b), 29, 32	5 I c), 5 I e), 17, 22, 25, 40 II d)	5 I a), 13, 14, 15, 19, 25, 30, 32, 33, 40, 42	5 I d),5 I f), 13 II c), 14 II d), 15 I e), 16, 17, 18, 20, 21, 25, 32

Tabelle 4: Zuordnung der Erwägungsgründe der DS-GVO zu den Gewährleistungszielen.

Datenminimierung	*Verfügbarkeit*	*Integrität*	*Vertraulichkeit*	*Nichtverkettung*	*Transparenz*	*Intervenierbarkeit*
28, 29, 30, 39, 78, 156	49, 78, 83	39, 49, 78, 83	39, 49, 78, 83	31, 32, 33, 39, 50, 53, 71, 78	32, 39, 42, 58, 60, 61, 63, 74, 78, 84, 85, 86, 87, 90, 91, 100	39, 59, 65, 66, 67, 68, 69, 70, 78

7 Die generischen Maßnahmen zur Umsetzung der Gewährleistungsziele

Für jede der Komponenten des SDMs (Daten, Systeme und Prozesse) werden für jedes der Gewährleistungsziele im Anhang Referenzmaßnahmen benannt und beschrieben. Für jede der Maßnahmen sind auch die Auswirkungen auf den Erreichungsgrad von anderen, von der Maßnahme nicht direkt betroffenen Gewährleistungsziele zu betrachten. So können bestimmte Einzelmaßnahmen zur Erreichung mehrerer Gewährleistungszielen beitragen.

In diesem Abschnitt werden generische Datenschutz-Schutzmaßnahmen 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 Maßnahmenkatalog (im Anhang) wieder.

7.1 Datenminimierung

Das Gewährleistungsziel Datenminimierung kann erreicht werden durch:

- Reduzierung von erfassten Attributen der betroffenen Personen,
- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten,
- Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten,
- Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen,
- Implementierung automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren,
- Regelungen zur Kontrolle von Prozessen zur Änderung von Verfahren.

7.2 Verfügbarkeit

Typische Maßnahmen zur Gewährleistung der Verfügbarkeit sind:

- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß eines getesteten Konzepts,
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt),
- Dokumentation der Syntax der Daten,
- Redundanz von Hard- und Software sowie Infrastruktur,
- Umsetzung von Reparaturstrategien und Ausweichprozessen,
- Vertretungsregelungen für abwesende Mitarbeiter.

7.3 Integrität

Typische Maßnahmen zur Gewährleistung der Integrität bzw. zur Feststellung von Integritätsverletzungen sind:

- Einschränkung von Schreib- und Änderungsrechten,
- Einsatz von Prüfsummen, elektronische Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptokonzepts,
- dokumentierte Zuweisung von Berechtigungen und Rollen,
- Prozesse zur Aufrechterhaltung der Aktualität von Daten,
- Festlegung des Sollverhaltens von Prozessen und regelmäßiges Durchführen von Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen,
- Festlegung des Sollverhaltens von Abläufen bzw. Prozessen und regelmäßiges Durchführen von Tests zur Feststellbarkeit bzw. Feststellung der Ist-Zustände von Prozessen.

7.4 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,
- Implementierung eines sicheren Authentisierungsverfahrens,
- 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 das Verfahren ausgestattete Umgebungen (Gebäude, Räume)
- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen etc.),
- Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept),
- Schutz vor äußeren Einflüssen (Spionage, Hacking).

7.5 Nichtverkettung

Typische Maßnahmen zur Gewährleistung der Nichtverkettung sind:

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten,
- programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten,

- regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung,
- Trennung nach Organisations-/Abteilungsgrenzen,
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentisierungsverfahrens,
- Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle,
- Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten,
- geregelte Zweckänderungsverfahren.

7.6 Transparenz

Typische Maßnahmen zur Gewährleistung der Transparenz sind:

- Dokumentation von Verfahren insbesondere mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Verfahrensbeschreibungen, Zusammenspiel mit anderen Verfahren,
- Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verfahren,
- Dokumentation der Verträge mit den internen Mitarbeitern, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen,
- Dokumentation von Einwilligungen und Widersprüchen,
- Protokollierung von Zugriffen und Änderungen,
- Nachweis der Quellen von Daten (Authentizität),
- Versionierung,
- Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts,
- Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept.

7.7 Intervenierbarkeit

Typische Maßnahmen zur Gewährleistung der Intervenierbarkeit sind:

- differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten,
- Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen,
- dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verfahren sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes,

- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem,
- Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen,
- Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte,
- Einrichtung eines Single Point of Contact (SPoC) für Betroffene,
- operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten.

8 Die Verfahrenskomponenten

Der Begriff „Verfahren“ wird benutzt, um vollständige Datenverarbeitungsvorgänge zu beschreiben. Unter Datenverarbeitung fällt insbesondere jedes Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen, Nutzen, Anonymisieren, Pseudonymisieren und Verschlüsseln personenbezogener Daten. Ein Verfahren beschreibt eine formalisierte, wiederholbare Folge dieser oben genannten Schritte der Datenverarbeitung zur Umsetzung einer Fachaufgabe bzw. eines Geschäftsprozesses. Dabei ist gleichgültig, ob sie manuell oder mit Hilfe von Informationstechnik ausgeführt werden. Ein Verfahren ist immer gekennzeichnet durch seine Zweckbestimmung und wird dadurch von anderen Verfahren abgegrenzt.

Bei der Modellierung eines Verfahrens mit Personenbezug sind die folgenden drei Komponenten zu unterscheiden, weil diese auf der Ebene von Maßnahmen unterschiedliche Beiträge zur Umsetzung der Gewährleistungsziele leisten:

- die personenbezogenen Daten,
- die beteiligten technischen Systeme (Hardware, Software und Infrastruktur) sowie
- die organisatorischen und personellen Prozesse der Verarbeitung von Daten mit den Systemen.

Methodisch stehen zunächst die Daten von Personen im Vordergrund, deren Schutzbedarf durch die verantwortliche Stelle festzustellen bzw. festzusetzen ist. Diesen Schutzbedarf erben die Systeme und Prozesse. Anhand des Referenz-Schutzmaßnahmenkatalogs kann überprüft werden, ob getroffene oder geplante Schutzmaßnahmen eines Verfahrens dem Schutzbedarf angemessen sind.

Bei diesen drei Kernkomponenten spielen u. a. folgende Eigenschaften eine wesentliche 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 (bspw. alter, vermeintlich gelöschter Datenbestand einer Textdatei, der im Ausdruck nicht erscheint; Metadaten bspw. bzgl. Kameramodell, Ort und Zeit der Grafikdateien) oder wenn es sich um verlustbehaftete Dateien handelt (bspw. Grafik-, Video- und Audiodateien, in denen relevante Informationen der Kompression zum Opfer fallen können).

Bei den beteiligten Systemen sind *Schnittstellen* zu betrachten, die die Systeme zu anderen Systemen, die nicht innerhalb der vom Zweck definierten Systemgrenze liegen, unterhalten. Der Ausweis der Existenz von Schnittstellen sowie die Dokumentation von deren Eigenschaften sind von entscheidender Bedeutung zur Beherrschbarkeit und Prüfbarkeit von Datenflüssen.

Für jeden Prozess gilt es *Verantwortlichkeiten* zu klären, die typischerweise als Rollen in einem umfassenden Rollenkonzept formuliert und zugewiesen sind. Die Verantwortlichkeit eines Prozesseigentümers erstreckt sich auf Kernprozesse und Hilfsprozesse im Bereich von Technik und organisatorischen Regelungen oder im Bereich der inhaltlich geprägten Datenverarbeitung oder durchgängig über alle Prozessebenen eines Verfahrens hinweg im Sinne einer Gesamtverfahrensverantwortlichkeit. Diese Verantwortlichkeit kann auf unterschiedliche Rollen verteilt werden. Der Bezug von Prozess- und Verfahrensverantwortlichkeit ist von entscheidender Bedeutung für die Zuordnung, welche beteiligte Instanz für die Ordnungsmäßigkeit eines Verfahrens zur Datenverarbeitung aktiv zu sorgen hat.

Gerade bei der Betrachtung der Prozess- und Verfahrensverantwortlichkeit ist zu berücksichtigen, dass die Verfahrenskomponenten als Teile eines organisationsweiten Verfahrens oder jedoch als eigenständige Teilprozesse eingestuft werden können. In beiden Fällen müssen die Zuweisungen der Verantwortlichkeiten erkennbar sein.

9 Der Schutzbedarf

Jede Verarbeitung personenbezogener Daten durch eine Organisation stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Das betrifft auch solche Verarbeitungen, die aus datenschutzrechtlicher Sicht zulässig sind, also auf der Basis einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung erfolgen. Eine Organisation muss deshalb nachweisen, dass sie diesen Eingriff auf das erforderliche Maß beschränkt, die Eingriffsintensität also minimiert (siehe bspw. Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO). Diesen Nachweis kann sie erbringen indem sie darstellt, auf welche Weise sie die Gewährleistungsziele umsetzt.

Mit dem Begriff „Organisation“ werden in diesem Modell sowohl öffentliche Stellen, Privatunternehmen und andere Einrichtungen wie etwa wissenschaftliche Institute bezeichnet. Der Begriff „Organisation“ umfasst sowohl die verantwortliche Stelle als auch den Auftragnehmer im Rahmen einer Auftragsdatenverarbeitung im Sinne des deutschen Datenschutzrechts bzw. den Controller und den Processor im Sinne der Datenschutz-Grundverordnung (DS-GVO).

Bei der Ermittlung des Schutzbedarfs nimmt das SDM die Perspektive des Betroffenen und dessen Grundrechtsausübung ein und unterscheidet sich daher von der Sicht des IT-Grundschutzes.

Der IT-Grundschutz hat vorrangig die Informationssicherheitsstandards im Blickfeld und soll in erster Linie die Daten verarbeitende Organisation schützen. Für die Festlegung des Schutzbedarfs nach dem SDM ist folgerichtig die *Eingriffsintensität* maßgeblich, die die Datenverarbeitung durch die Organisation für den Betroffenen darstellt.

9.1 Eingriffsintensität

Um den Schutzbedarf der Informationssicherheit bewerten zu können ist es methodisch üblich, Schadenshöhen und Eintrittswahrscheinlichkeiten zu erfassen und das daraus resultierende Risiko zu bewerten. Der Schutz (der Grundrechte) von Personen steht mit diesem Vorgehen jedoch nicht im Fokus dieser Methode. Um beurteilen zu können, wie groß die Risiken für das Recht auf informationelle Selbstbestimmung sind und welcher individuelle Schutzbedarf aus einem Verfahren resultiert, muss die Eingriffsintensität in die Grundrechte durch ein Verfahren beurteilt werden. Maß für die Eingriffsintensität ist dabei unter anderem der durch die entsprechende Rechtsgrundlage bestimmte Zweck der Datenverarbeitung, die Schutzbedürftigkeit, die Dauer der Speicherung, die Art und Anzahl möglicher Empfänger der verarbeiteten Daten. Die Anwendung des SDM kann somit zum Ergebnis haben, dass der Schutzbedarf für Geschäftsprozesse nicht mit dem Schutzbedarf für Betroffene übereinstimmt.

9.2 Die besondere Rolle des Gewährleistungsziels Vertraulichkeit

Eine besondere Rolle für die Bestimmung des Schutzbedarfs spielt das Gewährleistungsziel Vertraulichkeit. Die Vertraulichkeit personenbezogener Daten muss auch dann durch angemessene Maßnahmen gewährleistet sein, wenn die Eingriffstiefe in das Recht auf informationelle Selbstbestimmung gering ist. Hier ist der Überschneidungsbereich zwischen SDM und BSI-Grundschutzmethodik hoch. Die Anforderungen einer Organisation an die Sicherheit der eigenen IT-Infrastruktur decken sich zu großen Teilen mit den Anforderungen des Betroffenen an die Gewährleistung der Vertraulichkeit seiner Daten. Die Auswahl der Maßnahmen zum Schutz personenbezogener Daten deckt sich daher in weiten Bereichen mit der Auswahl der Maßnahmen, die die Anforderungen des Grundschutzes an eine angemessene Informationssicherheit sicherstellen sollen.

9.3 Schutzbedarfsabstufungen

Das SDM geht davon aus, dass ein Schutzbedarf in Bezug auf den Grundrechtseingriff, der allein durch die Verarbeitung von personenbezogenen Daten entsteht, klassifizierbar ist. Das SDM unterscheidet in Anlehnung an die IT-Grundschutz-Methodik des BSI die drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ für Verfahren zur Verarbeitung personenbezogener Daten.

Schutzbedarfskategorie „normal“

Da *jede* Verarbeitung personenbezogener Daten einen Eingriff in die Grundrechte der betroffenen Person darstellt, kann der Schutzbedarf gemäß SDM niemals niedriger als „normal“ sein. Deshalb ist grundsätzlich davon auszugehen, dass jedes personenbezogene Verfahren mindestens *normalen Schutzbedarf* aufweist. Weniger schutzbedürftig können folgerichtig nur Verarbeitungen mit nichtpersonenbezogenen Daten sein.

Schutzbedarfskategorie „hoch“

Folgende beispielhaft aufgeführte Verarbeitungsszenarien implizieren eine Eingriffsintensität, welche einen höheren als normalen Schutzbedarf zur Folge haben kann:

- Verarbeitung nicht veränderbarer Personen-Daten, die ein Leben lang als Anker für Profilbildungen dienen können bzw. zuordenbar sind (z. B. biometrische Daten, Gendaten),
- Verbreitung eindeutig identifizierender, hoch verknüpfbarer Daten (z. B. lebenslang gültige Krankenversichertennummer, Steuer-ID),
- gesetzlich begründete oder anderweitig zu erklärende Intransparenz der Verfahrensweisen für Betroffene (z. B. Verfassungsschutz, Schätzwerte im Scoring),
- Verarbeitung von Daten in einem Verfahren mit möglichen gravierenden, finanziellen Auswirkungen für Betroffene,
- Verarbeitung von Daten in einem Verfahren mit möglichen Auswirkungen auf das Ansehen/die Reputation des Betroffenen,
- Verarbeitung von Daten in einem Verfahren mit möglichen Auswirkungen auf die körperliche Unversehrtheit des Betroffenen,

- Verarbeitung von Daten, die realistischer Weise zu erwartende Auswirkungen auf die Grundrechtsausübung einer Vielzahl Betroffener haben können (z. B. bei zunehmend flächendeckender, öffentlicher Videoüberwachung),
- Gefahr von Diskriminierung, Stigmatisierung (z. B. durch Algorithmen, intransparentes Zustandekommen von Entscheidungen eines Betroffenen),
- Eingriffe in besonders geschützten inneren Lebensbereich eines Betroffenen.

Hoher Schutzbedarf für ein personenbezogenes Verfahren besteht darüber hinaus dann, wenn Betroffene von den Entscheidungen bzw. Leistungen einer Organisation abhängig sind (etwa in der. Leistungsverwaltung oder im medizinischen Bereich) und wenn eine Organisation

- mit einer weitreichenden Eingriffsintensität Daten verarbeitet, was zu erheblichen Konsequenzen für den Betroffenen führen kann,
- Daten verarbeitet, welche gesetzlich als besonders schutzwürdig ausgewiesen sind,
- keine real nachweislich funktionierenden Möglichkeiten der Intervention und des Selbstschutzes für Betroffene bereitstellt.

Ein hoher Schutzbedarf besteht auch dann, wenn es ist nicht möglich ist, dass Konflikte unter realistisch zu bewältigenden Bedingungen für den Betroffenen vor Gericht geklärt werden können (Bsp. Anbieter von Telekommunikationsdienstleitungen ohne Niederlassung vor Ort). Die DS-GVO versucht dieses Problem durch Einführung des Marktortprinzips zu lösen.

In einigen Fällen hat schon der Gesetzgeber im Gesetzestext den Schutzbedarf explizit ausgewiesen. So enthält das BDSG in §§ 13 Abs. 2, 28 Abs. 6 bis 9 und 29 Abs. 5 Sonderregelungen für „besondere Arten personenbezogener Daten“. Diese Regelungen finden sich in teilweise gleichlautender Form auch in anderen Datenschutzgesetzen bzw. in der DS-GVO (bspw. Art. 35 Abs. 3). Wenn diese besonderen Arten personenbezogener Daten verarbeitet werden, bedarf es grundsätzlich keiner weiteren Abstimmung oder Erwägungen, sondern es ist von einem „hohen Schutzbedarf“ auszugehen.[1]

Schutzbedarfskategorie „sehr hoch“

Von *sehr hohem Schutzbedarf* ist auszugehen, wenn ein Betroffener von den Entscheidungen bzw. Leistungen der Organisation unmittelbar existentiell abhängig ist und zusätzliche Risiken für den Betroffenen nicht bemerkbar sind.

9.4 Kollision zwischen Informationssicherheits- und Grundrechts-Schutzbedarf

IT-Grundschutz nach BSI nutzt ebenfalls Schutzbedarfsfeststellungen. Wegen der unterschiedlichen Zielrichtungen von IT-Grundschutz und SDM kann nicht ausgeschlossen werden,

[1] Generell wäre es wünschenswert, wenn bei Gesetzesentwürfen darauf hingewirkt wird, dass der Schutzbedarf von Daten explizit festlegt wird.

dass die Schutzbedarfsfeststellung nach Grundschutz und nach SDM für dieselbe Verarbeitung unterschiedlich ausfallen. Allerdings gelten auch beim IT-Grundschutz personenbezogene Daten als besonders schutzbedürftig. Da die Informationssicherheit auch von grundrechtlichen Erwägungen geleitet sein muss, müsste eine korrekt durchgeführte Schutzbedarfsbetrachtung nach IT-Grundschutz zu gleichen Ergebnissen kommen wie die Schutzbedarfsbetrachtung nach SDM.

Sollte es ausnahmsweise dennoch zu unterschiedlichen Urteilen kommen, muss die Schutzbedarfsfeststellung nach den datenschutzrechtlichen Prinzipien des SDM den Vorrang haben. Das solche unterschiedlichen Bewertungen nicht ausgeschlossen werden können zeigt das folgende Beispiel: Die Protokollierung des Verhaltens von Mitarbeiterinnen und Mitarbeitern oder die Beobachtung externer Nutzer zur Abwehr von Informationssicherheitsangriffen kann aus Datenschutzsicht anders bewertet werden als aus der Sicht der Informationssicherheit. Solche Fälle sind hinsichtlich der Festlegung des Schutzbedarfs besonders zu behandeln, zu dokumentieren und zu ggf. rechtfertigen.

9.5 Kumulierungseffekte

Der Schutzbedarf ist für unter Punkt 8 bereits beschriebenen Komponenten Daten, Systeme und Prozesse zu betrachten. Es hat sich in der Praxis methodisch bewährt, zunächst mit Blick auf den Verarbeitungszweck den Schutzbedarf der Daten zu ermitteln, der sich dann auf Systeme und Prozesse, als weitere Komponenten eines Verfahrens, vererbt. Dabei sind zwei Typen von Kumulierungseffekte zu beachten:

- Daten, die normalen Schutzbedarf aufweisen, können hohen Schutzbedarf erfordern, wenn sie in großer Menge verarbeitet werden („Kumulierung vieler Daten“).
- Daten, die normalen Schutzbedarf aufweisen, können hohen Schutzbedarf erfordern, wenn sie von Personen verarbeitet werden, die zu verschiedenen Zwecken unterschiedliche Rollen mit unterschiedlichen Rechten einnehmen („Kumulierung vieler Rechte“).

9.6 Risikoanalyse

Neben einer Betrachtung des Eingriffs in die Grundrechte ist eine Risikoanalyse notwendig, in deren Ergebnis beurteilt werden soll, wie groß die Wahrscheinlichkeit ist, dass die betreffende Organisation trotz aller getroffenen Maßnahmen zum Schutz der Grundrechte Datenschutzvorgaben nicht einhalten wird. Aus dieser Risikoanalyse können sich zusätzliche Schutzmaßnahmen ergeben, die die aus der Eingriffsintensität resultierenden Maßnahmen ergänzen.

Eine solche Datenschutz-Risikoanalyse kann auch solche Aspekte der Informationssicherheit betreffen, die der Abwehr von unbefugten sowie integritätsgefährdenden Zugriffen auf personenbezogene Daten – auch zum Schutze der Betroffenen – dienen. Die Datenschutz-Risikoanalyse betrachtet auch die Organisationen, die Daten befugt verarbeiten. Dabei sind insbesondere die folgenden vier Aspekte zu erfassen und zu beurteilen:

1. Es ist die Stärke der Motivation einer Organisation zu beurteilen, den *Zweck* der Nutzung von Daten unbefugt *zu ändern*.
2. Es sind die *operativen Möglichkeiten* zu beurteilen, die für eine Organisation bestehen, den Zweck der Datenverarbeitung unbefugt zu ändern, sofern die Motivation einer solchen Zweckänderung gegeben ist.
3. Es sind Auswirkungen von Übermittlungen personenbezogener Daten *in Drittstaaten* zu beachten. Unabhängig vom jeweils festgestellten Schutzbedarf der Daten im nationalen Kontext müsste geprüft werden, welche zusätzlichen Schutzmaßnahmen für die Übermittlung und ggf. Verarbeitung in Drittstaaten erforderlich wären.
4. Es ist das *Maß der getroffenen Schutzmaßnahmen der Informationssicherheit* zu beurteilen einschließlich der Prozesse zur Lösung von Konflikten zwischen Sicherung der Informationssicherheit der Geschäftsprozesse und zur operativen Sicherung des Datenschutzrechts betroffener Personen.

9.7 Allgemeine Vorgehensweise bei hohem Schutzbedarf

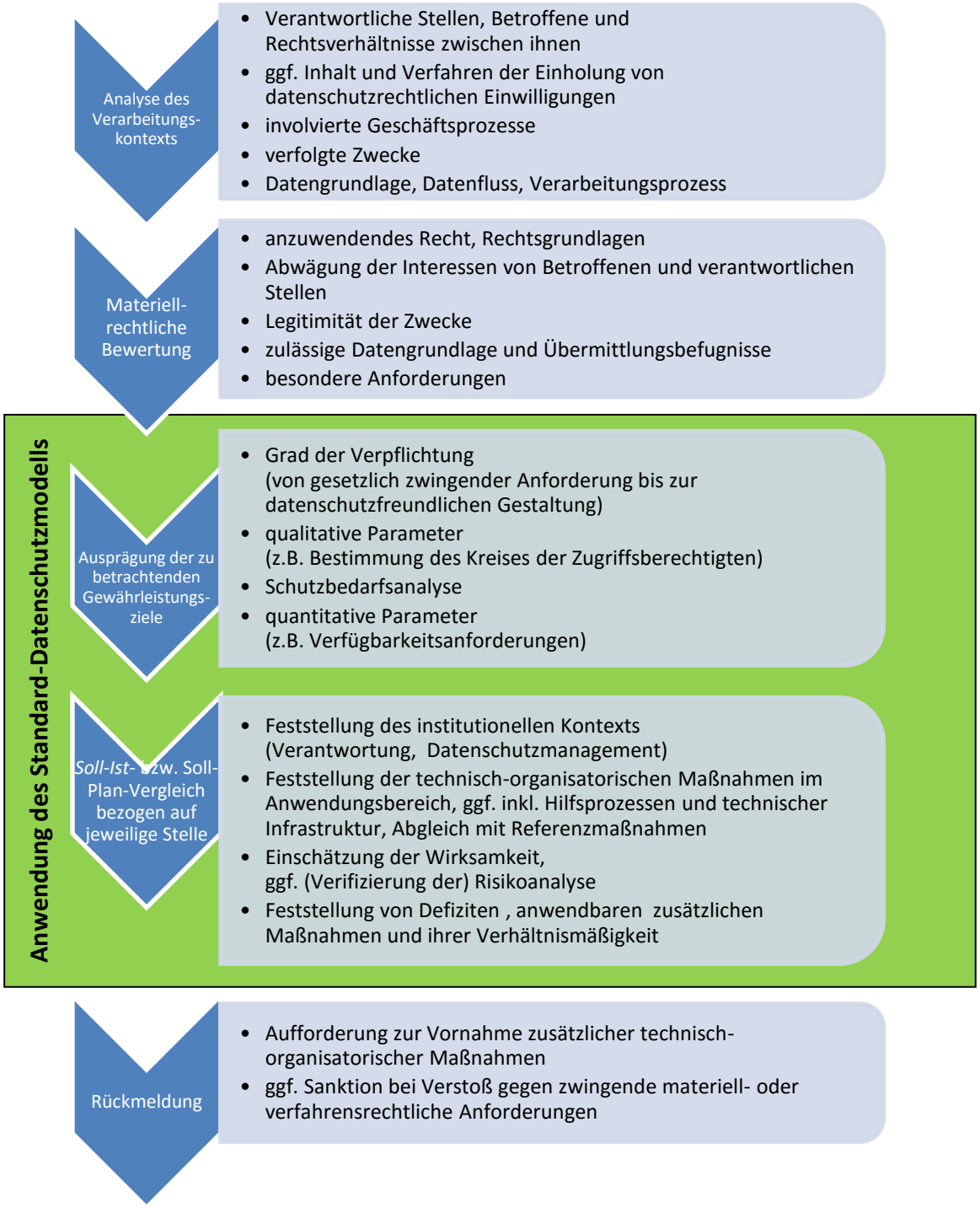
Ein hoher Schutzbedarf hat oft zur Folge, dass zusätzliche Maßnahmen ergriffen werden müssen, um die Gewährleistungsziele zu erreichen. Geeignete Maßnahmen sind in den jeweiligen Bausteinen des Maßnahmenkatalogs angegeben. Gleichzeitig müssen die für normalen Schutzbedarf geeigneten Maßnahmen fortgeführt und ihre Ausführung an den Schutzbedarf angepasst werden.

Dies kann zum einen dadurch geschehen, dass die Wirkung einer Maßnahme erhöht wird, soweit sie einen Ansatzpunkt für eine derartige Skalierung bietet. Ein Beispiel hierfür ist die Erhöhung der Länge eingesetzter kryptografischer Schlüssel. Zum anderen kann die Anpassung dadurch erfolgen, dass mit größerer Zuverlässigkeit eine spezifikationsgerechte Ausführung der Maßnahme sichergestellt wird. Dazu müssen mögliche Störeinflüsse – technische Fehler, Fehlverhalten von Nutzern, höhere Gewalt und äußere Einwirkung – bestimmt und die Robustheit der Maßnahme durch zusätzliche Vorkehrungen – oft organisatorischer Natur – erhöht werden.

Dieser iterative Prozess ist soweit fortzuführen, bis Gefährdungen der Gewährleistungsziele mit für den jeweiligen Schutzbedarf ausreichender Zuverlässigkeit ausgeschlossen werden. Der Nachweis für diese Wirkung ist in der Risikoanalyse zu dokumentieren.

10 Prüfen und Beraten auf der Grundlage des Standard-Datenschutzmodells

In dem folgenden Abschnitt sollen Hinweise zur Nutzung des Standard-Datenschutzmodells in Prüf- und Beratungsvorgängen der Datenschutzbehörden gegeben werden.



Die Abbildung 1: Anwendung des Standard-Datenschutzmodells im Rahmen von Prüf- und Beratungsvorgängen

Eine nutzbringende Anwendung des Modells setzt voraus, dass zuvor Klarheit über die mit dem Vorgang verfolgte Zielstellung gewonnen wurde. In den seltensten Fällen prüft eine Datenschutzbehörde die Datenverarbeitung einer verantwortlichen Stelle umfassend. Auch Beratungsersuchen fokussieren in aller Regel auf spezifische Aspekte eines Verfahrens oder des Einsatzes einer Technologie. Prüf- bzw. Beratungsgegenstände sind sowohl in Bezug auf die einzubeziehenden Sachverhalte als auch die zu berücksichtigenden Anforderungen begrenzt. In der Folge ist auch ggf. eine Auswahl der in den Gewährleistungszielen verkörperten gesetzlichen Anforderungen zu treffen, die im Vorgang betrachtet werden sollen. Dies wird im Weiteren vorausgesetzt.

Eine Übersicht über eine zweckmäßige Vorgehensweise bei der Anwendung des SDM wird in Abbildung 1 gegeben. In Beratungsvorgängen kann sich die Notwendigkeit ergeben, zyklisch vorzugehen und einzelne Phasen mehrfach in dem Maße zu durchlaufen, wie der Verarbeitungskontext an die Erfordernisse des Datenschutzes angepasst wird.

Für die Anwendung des SDM bestehen zwei Voraussetzungen: Erstens Klarheit über die sachlichen Verhältnisse, im Rahmen derer die zu betrachtende Datenverarbeitung stattfindet bzw. stattfinden soll, und zweitens eine materiellrechtliche Beurteilung dieser Verarbeitung.

Ausgehend von diesen Voraussetzungen und dem Ziel des Beratungs- oder Prüfungsvorgangs kann bestimmt werden, in welcher Ausprägung die Gewährleistungsziele anzuwenden und im Vorgang zu betrachten sind und wie hoch der Schutzbedarf in den einzelnen Dimensionen des Modells ist. In Anwendung des Modells kann hieraus ein Satz von technischen und organisatorischen Referenzmaßnahmen abgeleitet werden, mit denen die vorgesehenen bzw. in der Prüfung festgestellten Maßnahmen verglichen werden können. Zu diesem Vergleich gehört auch die Bestimmung, inwieweit Defizite der Anwendung der Referenzmaßnahmen durch alternative Maßnahmen ausgeglichen werden. Am Abschluss steht eine Bewertung der verbleibenden Restrisiken für die informationelle Selbstbestimmung der Betroffenen und ggf. der Wege, diese mit verhältnismäßigen zusätzlichen Maßnahmen auf ein akzeptables Maß zu mindern.

Diese im Ergebnis der Anwendung des Modells getroffene Bewertung kann in der Folge Grundlage für die Empfehlung bzw. die Aufforderung bilden, technische oder organisatorische Mängel zu beheben bzw. von der Verarbeitung Abstand zu nehmen, soweit sich eine ausreichende Risikominderung mit verhältnismäßigen Mitteln nicht erreichen lässt.

Die vorgenannten Schritte werden im Weiteren näher betrachtet.

10.1 Vorbereitung

Sowohl die materiellrechtliche Bewertung als auch die Anwendung des SDM zur Beurteilung der vorgenommenen oder geplanten technischen und organisatorischen Maßnahmen basieren auf der Feststellung der sachlichen Verhältnisse der Verarbeitung. Hierzu gehören insbesondere die Fragen:

- Wer trägt die Verantwortung?
- Erfolgt die Verarbeitung zur Erfüllung der Aufgabe einer öffentlichen Stelle?
- Besteht ein rechtsgeschäftliches oder rechtsgeschäftsähnliches Schuldverhältnisses einer verantwortlichen privaten Stelle mit den Betroffenen?
- Bilden Einwilligungen der Betroffenen die Rechtsgrundlage der Verarbeitung und, wenn ja, welchen Inhalt haben sie und wie werden sie eingeholt?
- Wenn mehrere verantwortliche Stellen oder Auftragsdatenverarbeiter in die Verarbeitung involviert sind, wie sind dann die Rechtsverhältnisse zwischen ihnen geregelt?
- Für welche Zwecke erfolgt die Verarbeitung und welche Geschäftsprozesse der verantwortlichen Stelle(n) werden durch sie unterstützt?
- Welche Daten werden in welchen Schritten und unter Nutzung welcher Systeme und Netze und der Kontrolle welcher Personen erhoben, verarbeitet und genutzt?
- Welche Hilfsprozesse werden zur Unterstützung der Verarbeitung betrieben?
- Welche technische Infrastruktur wird genutzt?

Ausführlichkeit und Detaillierungsgrad der Feststellung der sachlichen Verhältnisse werden von Vorgang zu Vorgang 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 dennoch ebenso üblich wie für die weiteren Schritte unentbehrlich.

Die sich an die Feststellung der sachlichen Verhältnisse anschließende materiellrechtliche Bewertung beurteilt, inwieweit die geprüfte oder vorgesehene Verarbeitung grundsätzlich zulässig ist. Darüber hinaus gibt sie Antworten auf folgende Fragen, die für die folgende Anwendung des SDMs relevant sind:

- Welches Recht ist auf die Verarbeitung anzuwenden?
- Welche Zwecke können mit der Verarbeitung legitim verfolgt werden und welche Zweckänderungen sind im Zuge der Verarbeitung zulässig?
- Welche Daten sind für die Erfüllung der zulässigen Zwecke erheblich bzw. erforderlich?
- Welche Befugnisse bestehen zur Übermittlung von Daten zwischen den beteiligten Stellen und von diesen an Dritte?
- Welchen Beschränkungen unterliegt die Offenbarung von verarbeiteten Daten an Personen innerhalb und außerhalb der beteiligten Stellen?
- Welchen besonderen Anforderungen müssen die technischen und organisatorischen Maßnahmen genügen?

Die letztgenannten besonderen Anforderungen können sich zum einen aufgrund spezialgesetzlicher Regelung ergeben. Zum anderen kann die Situation eintreten, dass nur mit Erfüllung dieser Anforderungen im Rahmen der Interessensabwägung von einem Zurücktreten der Interessen der Betroffenen am Ausschluss der Verarbeitung ausgegangen werden kann.

10.2 Ausprägung der Gewährleistungsziele

In welcher Ausprägung die Gewährleistungsziele für die betrachtete Datenverarbeitung zu formulieren sind, hängt zunächst davon ab, welches Recht auf die Verarbeitung anzuwenden ist – die Kontrollkataloge des BDSG und einer Reihe von LDSG oder die Schutzzielkataloge der anderen LDSG – und ob die Anwendung des SDM im Rahmen einer Prüfung erfolgt oder im Rahmen einer Beratung, bei der über die Einhaltung der gesetzlichen Minimalanforderungen hinaus auch auf eine datenschutzfreundliche Gestaltung hingewirkt werden soll.

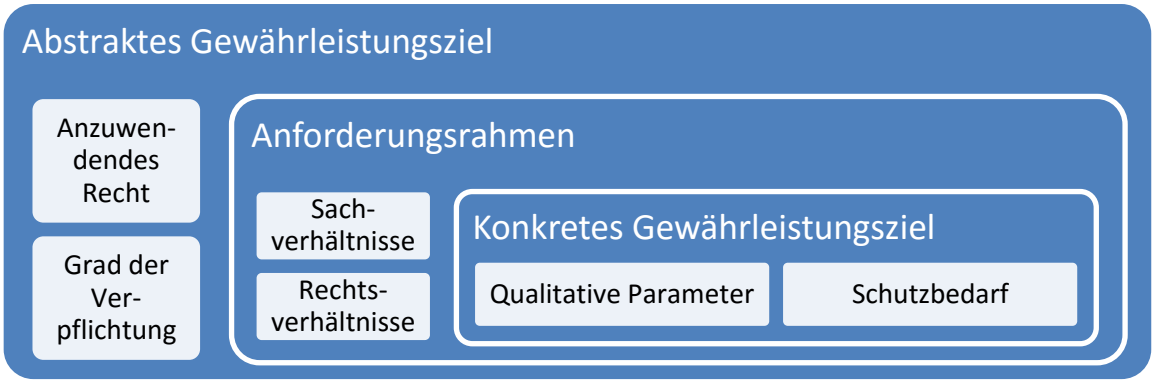


Abbildung 1: Ausprägung der Gewährleistungsziele

Ausgehend von der gewählten Ausprägung sind die zu betrachtenden Gewährleistungsziele qualitativ und nach Möglichkeit technikneutral näher zu bestimmen:

1. *Innerhalb von welchen Prozessen ist für wen die Verfügbarkeit von welchen Daten zu gewährleisten?* Der Einfluss der Möglichkeit der ordnungsgemäßen Verwendung der Daten auf die Interessen der Betroffenen ist der Maßstab für die Konkretisierung des Gewährleistungsziels der Verfügbarkeit. Das Gewährleistungsziel erstreckt sich nur auf solche Daten und diejenigen Geschäftsprozesse, bei denen ein Verlust der Verfügbarkeit den Interessen der Betroffenen zuwiderläuft.
2. *Welche Daten sollen unversehrt, welche aktuell gehalten werden?* Auch hier ist das Interesse der Betroffenen der Maßstab. In Bezug auf die Gewährleistung der Aktualität ist in die Abwägung einzubeziehen, dass Aktualität in der Regel nur mit zusätzlichen Erhebungs- und Verarbeitungsvorgängen zu erhalten sein wird, deren Durchführung u. U. anderen Interessen der Betroffenen zuwiderlaufen können.
   Inwieweit die Integrität der Prozesse und Systeme zu gewährleisten ist, leitet sich aus der Konkretisierung der anderen Gewährleistungsziele ab.
3. *Wem ist die Kenntnisnahme welcher Daten zu verwehren?* 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 der verantwortlichen Stellen zu bewegen haben. Der Rahmen für die Kenntnisnahme Dritter ist durch die in der materiell-rechtlichen Analyse festgestellten Übermittlungsbefugnisse gegeben.

4. *Für wen ist die Datenverarbeitung in welcher Form transparent zu halten?* Es sind Anforderungen an die Verfahrensdokumentation nach § 4e BDSG, an die interne Dokumentation der Verarbeitungsvorgänge und deren Auswertbarkeit sowie an die Revisionsfähigkeit der Verarbeitung festzuhalten.
5. *Welche Betroffenenrechte sind in welcher Ausprägung zu gewähren?* Welche Betroffene müssen von der automatisierten Verarbeitung benachrichtigt werden? Welche Daten sind in die Beauskunftung unter welchen Bedingungen einzubeziehen? Unter welchen Bedingungen sind die Daten zu löschen bzw. zu sperren?
6. *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 Stellen 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.
7. *Die Kenntnisnahme von und die Ausübung welcher Verfügungsgewalt über welche Daten der Betroffenen durch welche Personen und Stellen sind zu minimieren?* Ausgangspunkt sind erneut die Interessen der Betroffenen, auch innerhalb einer Verarbeitung zu legitimen Zwecken die Belastung auf das erforderliche Maß zu begrenzen.

Nachdem die Gewährleistungsziele qualitativ feststehen, muss eine Schutzbedarfsanalyse erfolgen bzw. die Schutzbedarfsanalyse der verantwortlichen Stelle(n) nachvollzogen werden. Die Vorgehensweise ist in Kapitel 9 niedergelegt. 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 die verantwortliche Stelle in der Lage sein, die jeweiligen Betroffenenrechte zu gewähren?

Zum Zweiten bildet das Ergebnis der Schutzbedarfsanalyse die Grundlage für die Abwägung zwischen der Wahrung der Interessen der Betroffenen und dem hierfür erforderlichen Aufwand der verantwortlichen Stelle(n). Für typische Verarbeitungskontexte ist das Ergebnis einer solchen Abwägung durch die Darstellung regelhaft zu ergreifender Referenzmaßnahmen in Kapitel 7 vorgezeichnet.

Zum Dritten fließt das Ergebnis der Schutzbedarfsanalyse 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 hängen regelmäßig von dem Interesse von Dritten oder von Verfahrensbeteiligten ab, 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 erheben, zu nutzen, zu speichern, zu übermitteln oder anderweitig zu verarbeiten.

10.3 Der Soll-Ist-Vergleich

Der Kern der Anwendung des Standard-Datenschutzmodells besteht in dem Vergleich der Referenzmaßnahmen, die sich aus den betrachteten und wie oben konkretisierten Gewährleistungszielen ableiteten lassen, mit den von der verantwortlichen Stelle geplanten bzw. in der Prüfung festgestellten Maßnahmen. Abweichungen sind danach zu gewichten und zu beurteilen, inwieweit sie das Erreichen der Gewährleistungsziele gefährden. In einem Prüfvorgang 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, dass Anforderungen nicht erfüllt werden, weil die entsprechend zugeordneten Maßnahmen sofort ersichtlich fehlen. Komplizierter ist der Fall, wenn die zu prüfende Stelle andere als die Referenzschutzmaßnahmen gewählt hat. Auch wenn diese als grundsätzlich geeignet beurteilt werden können, müsste separat geprüft werden, ob sie in ihrer konkreten Ausgestaltung tatsächlich dem festgestellten Schutzbedarf entsprechen. An dieser Stelle hilft das SDM, die Erörterung auf den Nachweis dessen zu fokussieren, dass (oder inwieweit) die getroffene Schutzmaßnahme funktional äquivalent zur Referenzmaßnahme ist.

11 Das Betriebskonzept zum Standard-Datenschutzmodell

11.1 Einleitung

Das Betriebskonzept verfolgt den Zweck, den Anwendern dieses Modells Handlungssicherheit im Umgang zu geben. Das bedeutet zu klären, wer für das SDM einsteht, welche Version die aktuell gültige ist und zu welchem Zeitpunkt welche Version galt und wo diese aktuelle Version beziehbar ist. Das Betriebskonzept regelt drei Aspekte:

- Klärung der Rollen und Zuständigkeiten in Bezug zum Modell,
- Sicherstellung der Anwendbarkeit des SDM,
- Schaffung von Transparenz hinsichtlich der Veröffentlichung und Weiterentwicklung des Modells.

11.2 Auftraggeber, Projektleitung, Anwender

Der Auftraggeber für die Entwicklung und Pflege des SDM sind die Mitglieder der *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz - DSK).* Die DSK ist die Eigentümerin des SDM, das sowohl die Methodik als auch den Referenzmaßnahmenkatalog umfasst, und gibt dieses heraus.

Die Entwicklung und Pflege des SDM geschieht durch den *Arbeitskreis Technik* der DSK (AK Technik). Der AK Technik hat die Projektleitung inne.

Das SDM kann sowohl von den sechzehn Landesdatenschutzbeauftragten, dem Bayerischen Landesamt für Datenschutzaufsicht sowie der Bundesdatenschutzbeauftragte im Rahmen ihrer gesetzlichen Beratungs-, Prüf- und Sanktionstätigkeiten *(Anwendergruppe 1)* als auch von den verantwortlichen Stellen (dort insbesondere von den behördlichen und betrieblichen Datenschutzbeauftragten) bei der Planung und beim Betrieb von Verfahren zur Verarbeitung personenbezogener Daten *(Anwendergruppe 2)* angewendet werden.

Das Modell wird sowohl im Rahmen der Praxisevaluierung als auch gemäß fachlichen Erfordernissen wie folgt weiterentwickelt:

- Erstellung und Pflege des SDM, das auch den Katalog von Referenz-Schutzmaßnahmen umfasst;
- Bereitstellung des SDM und des Maßnahmenkatalogs;
- Bearbeitung von Änderungsanträgen (Change-Requests, CRs) zum SDM, die von beiden Anwendergruppen eingebracht werden können, über deren Annahme die DSK entscheidet;
- Sicherung der Qualität der Arbeitsergebnisse;
- Versionierung des SDM;
- Projektmanagement, das umfasst
    - Bereitstellung eines Single Point Of Contact (Service Desk);
    - Betrieb von CR-Verfolgung;

    - Moderation von Diskussionen;
    - Verwaltung der nötigen Betriebsmittel (Webseite, Projektplattform);
- Öffentlichkeitsarbeit.

12 Maßnahmenkatalog

Der Maßnahmenkatalog wird künftig Bestandteil des SDM, wird aber – in Abhängigkeit der technischen Entwicklung – in kürzeren Zyklen nach den Vorgaben des Betriebsmodells (siehe Kapitel 11) überarbeitet als das SDM selbst.

13 Stichwortverzeichnis