Das Standard-Datenschutzmodell

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

V.1.1 – Erprobungsfassung

von der 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 25./26. April 2018 in Düsseldorf einstimmig beschlossen

IMPRESSUM

Das Standard-Datenschutzmodell
Eine Methode zur Datenschutzberatung und -prüfung
auf der Basis einheitlicher Gewährleistungsziele

V.1.1 – Erprobungsfassung
von der 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 25./26. April 2018 in Düsseldorf einstimmig beschlossen

Eigentümer:
Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

Herausgeber:
AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

Redaktion:
UAG „Standard-Datenschutzmodell“ des AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

Autoren:
- *Kirsten Bock (Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein)*
- *Walter Ernestus (Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit)*
- *Meike Kamp (Berliner Beauftragte für Datenschutz und Informationsfreiheit)*
- *Lars Konzelmann (Der Sächsische Datenschutzbeauftragte)*
- *Dr. Tino Naumann (Der Sächsische Datenschutzbeauftragte)*
- *Uwe Robra (Die Landesbeauftragte für den Datenschutz Niedersachsen)*
- *Martin Rost (Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein)*
- *Gabriel Schulz (Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern)*
- *Julia Stoll (Der Hessische Datenschutzbeauftragte)*
- *Dr. Ulrich Vollmer (Berliner Beauftragte für Datenschutz und Informationsfreiheit)*
- *Michael Wilms (Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen)*

Ansprechpartner:
Leiter des AK Technik:
Gabriel Schulz
Der Landesbeauftragte für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern
Schloss Schwerin, 19053 Schwerin
E-Mail: gabriel.schulz@datenschutz-mv.de
Telefon: 0385 59494 37

Leiter der UAG „Standard-Datenschutzmodell“:
Martin Rost
Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein
Holstenstraße 98, 24103 Kiel
E-Mail: uld32@datenschutzzentrum.de
Tel: 0431 98813 91

Das Standard-Datenschutzmodell

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

V.1.1 – Erprobungsfassung

von der 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 25./26. April 2018 in Düsseldorf einstimmig beschlossen

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. Sie schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. In den Artikeln 5, 12, 24, 25 und 32 finden sich grundlegende Anforderungen an die Verarbeitung personenbezogener Daten. Die DS-GVO fordert geeignete technische und organisatorische Maßnahmen, um die Risiken für die Rechte und Freiheiten natürlicher Personen ausreichend zu mindern. Das betrifft sowohl Maßnahmen zur Gewährleistung der Rechte Betroffener (Kapitel III DS-GVO), als auch Maßnahmen zur Umsetzung der Datenschutzgrundsätze (Art. 25 Abs. 1 DS-GVO), darunter zur Datenminimierung (Art. 25 Abs. 2 DS-GVO) und Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1). Das Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO) fordert zu einer sehr frühzeitigen Befassung des Verantwortlichen mit datenschutzrechtlichen Vorgaben bei der Planung von Verarbeitungen auf. Die DS-GVO verlangt ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 24 Abs. 1 Satz 2, Art. 32 Abs. 1 Satz 1 lit. d DS-GVO). Schließlich sieht die DS-GVO ein Kohärenzverfahren vor, das die unabhängigen Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet (Kapitel VII DS-GVO – Zusammenarbeit und Kohärenz). Insbesondere dieses Verfahren erfordert ein abgestimmtes, transparentes und nachvollziehbares 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. Die Einhaltung der Grundsätze muss nachweisbar sein („Rechenschaftspflicht“). 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. Das SDM überführt mit Hilfe dieser Gewährleistungsziele die rechtlichen Anforderungen der DS-GVO in die von der Verordnung geforderten technischen und organisatorischen Maßnahmen. Das SDM enthält im Anhang einen Referenzkatalog von technischen und organisatorischen Maßnahmen. Dieser Katalog kann herangezogen werden, um bei jeder einzelnen Verarbeitung sowohl durch den Verantwortlichen selbst als auch durch die Aufsichtsbehörde zu prüfen, ob das rechtlich geforderte Soll von Maßnahmen mit dem vor Ort vorhandenen Ist von Maßnahmen übereinstimmt. Das SDM und der Maßnahmenkatalog bieten zudem eine sehr gut geeignete Grund-

lage für die Planung und Durchführung der von der DS-GVO geförderten datenschutzspezifischen Zertifizierungen (Art. 42 DS-GVO) und der in bestimmten Fällen erforderlichen Datenschutz-Folgenabschätzung (Art. 35 DS-GVO).

Eine derartige Standardisierung unterstützt auch die in der Verordnung normierte Zusammenarbeit der Aufsichtsbehörden. Denn auch auf nationaler Ebene müssen die deutschen Datenschutzbehörden in zunehmendem Maße zusammenarbeiten und mit einheitlichen Beratungs- und Prüfkonzepten die Verarbeitung personenbezogener Daten begleiten. Das SDM als 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, Nichtverkettung 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 als auch für die verantwortlichen Stellen im Bereich der privaten Wirtschaft und im Bereich der öffentlichen Verwaltung 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 bei der Verarbeitung personenbezogener Daten.

Mit dem SDM wird eine Methode bereitgestellt, mit dem die Risiken der Rechte und Freiheiten, 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 Me-

thoden zur Minimierung des Risikos. Diese Methoden können in speziellen Anwendungskontexten selbstverständlich ihre Berechtigung haben.

2 Der Zweck des Standard-Datenschutzmodells

Mit dem Standard-Datenschutzmodell (SDM) wird ein Werkzeug bereitgestellt, mit dem die Auswahl und Bewertung technischer und organisatorischer Maßnahmen unterstützt wird, die sicherstellen und den Nachweis dafür erbringen, dass die Verarbeitung personenbezogener Daten nach den Vorgaben der DS-GVO erfolgt. Diese Maßnahmen müssen angemessen und geeignet sein, die Risiken für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen soweit einzudämmen, dass ein dem Risiko angemessenes Schutzniveau gewährleistet wird. Für jede Verarbeitung ist also zu prüfen, ob die personenbezogenen Daten durch eine angemessene Auswahl technischer und organisatorischer Maßnahmen so verarbeitet werden, dass die Rechte der Betroffenen gewahrt bleiben und die Sicherheit der Verarbeitung gewährleistet wird (Kapitel III der 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 und somit die Auswahl geeigneter Maßnahmen unterstützen.

Voraussetzung für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten ist erstens das Vorhandensein einer ausreichenden und tragfähigen Rechtsgrundlage (Zulässigkeit der Verarbeitung) und zweitens die Gewährleistung der Sicherheit der Datenverarbeitung. Es gelten die Verarbeitungsgrundsätze gem. Art. 5 DS-GVO und die Bedingungen für die Rechtmäßigkeit der Verarbeitung gem. Art. 6 DS-GVO. Die Prüfung des Vorliegens einer Rechtsgrundlage als Voraussetzung der Zulässigkeit der Verarbeitung muss vor der Anwendung des SDM erfolgen (siehe Ablaufmodell in Kapitel 10). Diese Prüfung sollte auch eine erste Bewertung des Risikos der Verarbeitung für die Rechte und Freiheiten der von der Verarbeitung Betroffener einschließen. Denn die Auswahl geeigneter Maßnahmen setzt die Kenntnis der vorhandenen Risiken voraus.

Anschließend ist kumulativ die zweite Voraussetzung der Rechtmäßigkeit der Verarbeitung zu überprüfen – die Frage, ob geeignete Maßnahmen zur Eindämmung des Risikos für die Rechte und Freiheiten der von Verarbeitung Betroffener umgesetzt wurden. Insofern ist das SDM Teil eines iterativen Prozesses der rechtlichen Bewertung sowie der Auswahl und Umsetzung von technischen und organisatorischen Maßnahmen. Das SDM bietet mit seinen Gewährleistungszielen eine Übersetzungshilfe vom Recht zur Technik und unterstützt den ständigen Dialog zwischen Juristen und Technikern. Dieser Prozess läuft während des gesamten Lebenszyklus einer Verarbeitung und kann somit die Forderung der DS-GVO nach regelmäßiger Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen z.B. zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d DS-GVO) unterstützen.

Der oben beschriebene iterative Prozess muss weit vor Beginn der Verarbeitung starten. Denn die DS-GVO fordert in Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Bereits bei den ersten Planungen einer Verarbeitungstä-

tigkeit mit personenbezogenen Daten müssen mögliche Risiken identifiziert und bewertet werden, um die Folgen der Verarbeitung beurteilen und bewerten zu können. Mit der Datenschutz-Folgenabschätzung (DSFA) bietet die DS-GVO in Art. 35 für besonders risikobehaftete Verarbeitungen ein Verfahren an, das die Prinzipien „Data Protection by Design“ und „Data Protection by Default“ mit stärkerer Methodik und höherem Detaillierungsgrad unterstützt. Das SDM bietet die geeignete Systematik, um eine DSFA korrekt und vollständig abzuarbeiten.

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

3 Der Anwendungsbereich des Standard-Datenschutzmodells

Der wesentliche Anwendungsbereich des Standard-Datenschutzmodells sind Planung, Einführung und Betrieb einzelner Verarbeitungen (engl. „processing operations“), mit denen personenbezogene Daten verarbeitet werden (personenbezogene Verarbeitungen, engl. „processing of personal data“) 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 DS-GVO fordert, für jede Verarbeitung personenbezogener Daten technische und organisatorische Maßnahmen auszuwählen und umzusetzen, die nach dem Stand der Technik und nach dem Risiko der Rechte und Freiheiten natürlicher Personen erforderlich und angemessen sind. Diese Datenschutzmaßnahmen werden als Teil der Datenverarbeitung betrachtet, einschließlich der mit ihnen selbst möglicherweise verbundenen Verarbeitung personenbezogener Daten. Dass es sich vielfach so verhalten muss zeigt sich am Beispiel der Protokollierung, die in der Regel als ein unmittelbarer Bestandteil einer Verarbeitung gilt.

Die Rechtsgrundlage kann konkrete Maßnahmen vorschreiben, die verarbeitungsspezifisch umzusetzen sind, z. B. etwa 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 geboten sind, um eine rechtskonforme Verarbeitung zu ermöglichen.

In beiden Fällen stehen neben diesen verarbeitungsspezifisch ergriffenen Datenschutzmaßnahmen auch solche, die bei der Verarbeitung übergreifend eingesetzt werden. Diese können 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 Verarbeitungstätigkeiten bieten.

Das SDM hat das Ziel, sowohl verpflichtende, wie auch optionale, sowohl verarbeitungsspezifische, als auch verarbeitungsübergreifende Datenschutzmaßnahmen zu systematisieren und ihre Bewertung zu ermöglichen. Dafür kann das SDM 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 der Verarbeitung personenbezogener Daten angewendet werden.

4 Die Struktur des Standard-Datenschutzmodells

Das Standard-Datenschutzmodell

- überführt datenschutzrechtliche Anforderungen in einen Katalog von Gewährleistungszielen,
- gliedert eine Verarbeitungstätigkeit in die Komponenten Daten, IT-Systeme und Prozesse,
- berücksichtigt die Einordnung von Daten in 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 Anforderungen den Begriff „Gewährleistungsziel“. Diese Anforderungen zielen auf Eigenschaften einer rechtskonformen Verarbeitung, die durch technische und organisatorische Maßnahmen „gewährleistet“ werden müssen. Die Gewährleistung besteht im Ausschluss von Abweichungen von einer rechtskonformen Verarbeitung. So ist eine Eigenschaft rechtskonformer Verarbeitung, dass sie nicht zu unberechtigter Kenntnisnahme führt, zum Beispiel durch Ausschluss einer unberechtigten Kenntnisnahme. Die Maßnahmen müssen daher gewährleisten, dass es zu einer unberechtigten Kenntnisnahme nicht kommen kann. Der Grad der zu erreichenden Zuverlässigkeit der Maßnahme ist Gegenstand einer Abwägung zwischen dem Risiko für die Rechte und Freiheiten natürlicher Personen und dem Aufwand unter Berücksichtigung des Stands der Technik. Die Verpflichtung, die Gewährleistungsziele durch technische und 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 gem. Art. 24, 25 und 32 DS-GVO 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) zur Vertraulichkeit und Integrität informationstechnischer Systeme herzustellen. Das Bundesverfassungsgericht hatte darin auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abgestellt.

5.2 Die zentralen datenschutzrechtlichen Anforderungen

Die folgenden datenschutzrechtlichen Anforderungen, die sowohl übergreifend in der DS-GVO als auch 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 Maß (Datenminimierung),
- die Berücksichtigung der Betroffenenrechte, wonach bei einer Verarbeitung Prozesse insbesondere für die Information über, die Auskunft zu, die Berichtigung, Löschung, Verarbeitungseinschränkung und Übertragbarkeit von Betroffenendaten vorzusehen sind,
- die Transparenz von Verarbeitungstätigkeiten als Voraussetzung dafür, dass die rechtlich festgelegten Anforderungen an eine Verarbeitung sowohl für die Organisation selber, als auch zumindest in einer allgemeinverständlichen Form für den Betroffenen sowie für die Aufsichtsbehörden überprüfbar sind,
- die Sicherheit der Verarbeitung der eingesetzten Komponenten zur Datenverarbeitung in Bezug auf die Rechte und Freiheiten natürlicher Personen (Art. 32 Abs. 1).

Das SDM betrachtet weder grundlegende Fragen der materiellen Rechtmäßigkeit einer Verarbeitung noch spezialgesetzliche Regelungen oder Regelungen auf einem hohen Detaillierungsgrad. Die Orientierung an den allgemein geltenden Gewährleistungszielen des Datenschutzes erübrigt daher nicht die Kenntnisnahme der datenschutzrechtlichen Regelungen, auch nicht im Bereich der technischen und 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, die Erhebung personenbezogener Daten und ihre Weiterverarbeitung auf das dem Zweck angemessene, erheblich und notwendige Maß zu beschränken (Art. 5 lit. c DS-GVO). Diese grundlegende Anforderung erfasst in Umsetzung des Zweckbindungsgrundsatzes 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 Notwendigkeit, 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 benötigt werden. Datenminimierung ist als proaktives Element datenschutzfreundlicher Technikgestaltung (Art. 25 DS-GVO) zu berücksichtigen: beginnend idealerweise beim Design der Informationstechnik durch den Herstel-

ler, über ihre Konfiguration und Anpassung an die Betriebsbedingungen, bis zu ihrem Einsatz in den Kernprozessen der Verarbeitung 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 Legitimität der Zwecksetzung sowie die Angemessenheit, Erheblich- und Notwendigkeit 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.

Ausgehend von der als zulässig bewerteten Zwecksetzung und Datengrundlage können 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. 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 und damit nicht mehr erforderlicher 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 Identifizierung der Betroffenen ermöglichen, können gelöscht oder transformiert (Anonymisierung, Pseudonymi-

sierung) oder ihre Anzeige in Datenmasken unterdrückt werden, so dass sie den handelnden Personen nicht zur Kenntnis gelangen, vorausgesetzt, diese Kenntnis ist für den jeweiligen Verarbeitungszweck entbehrlich.

5.4 Die elementaren Gewährleistungsziele

5.4.1 Die 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 informationstechnische 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. Integrität wird zudem als eine Form der Richtigkeit im Sinne des Art. 5 Abs. 1 lit. d DS-GVO verstanden, woraus der Anspruch resultiert, 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 der Verarbeitung und dessen Zwecksetzung insgesamt.

(3) Das Gewährleistungsziel *Vertraulichkeit* bezeichnet die Anforderung, dass keine unbefugte Person personenbezogene Daten 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 einer Verarbeitungstätigkeit 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 Verarbeitungstätigkeiten 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 technische und 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 Schutzzielen der IT-Sicherheit ein etwas erweitertes Verständnis, denn der Datenschutz nimmt zusätzlich eine darüber hinausgehende, erweiterte Schutz-Perspektive ein, indem er auch die Risiken betrachtet, die von den Aktivitäten der Organisation selbst innerhalb und außerhalb ihrer Geschäftsprozesse für die Rechte und Freiheiten natürlicher Personen bestehen. Methodisch gesprochen muss sich deshalb nicht nur eine Person gegenüber einer Organisation durch überprüfbare Eigenschaften als vertrauenswürdig ausweisen, sondern auch eine Organisation gegenüber einer betroffenen Person. Eine durchgeführte Datenschutzfolgenabschätzung (Art. 35 DS-GVO) in besondere Weise geeignet, diesen Nachweis zu erbringen.

Die folgenden, auf den spezifischen Schutzbedarf natürlicher Personen 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 personenbezogene Daten nicht zusammengeführt, also verkettet, werden dürfen. Eine Zusammenführung darf nur dann erfolgen, wenn die in Art. 5 Abs. 1 lit. b DS-GVO normierte Anforderung beachtet wird, dass Daten nur für den Zweck verarbeitet und ausgewertet werden, 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 können die Begehrlichkeiten sein, die Daten, über die ursprüngliche Rechtsgrundlage hinaus, zu nutzen. Rechtlich zulässig sind derartige Weiterverarbeitungen nur unter eng definierten Umständen. Art. 6 Abs. 4 DS-

GVO lässt Verarbeitungen nur zu auf Basis einer fortdauernden Einwilligung der Betroffenen nach Benachrichtigung, auf Basis einer Rechtsvorschrift für Zwecke nach Art. 23 Abs. 1 DS-GVO, für kompatible Zwecke, die nach den Kriterien des Art. 6 Abs. 4 DS-GVO bestimmt wurden, sowie insbesondere 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 in Art. 5 Abs. 1 lit. a DS-GVO genannte 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 bei einer Verarbeitungstätigkeit 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 Änderungen an der Verarbeitung 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.

6 Der Bezug der Gewährleistungsziele zum 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 ausgerichteten 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 Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme entwickelt. Un-

ter 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 der Nutzerin und des Nutzers auch hierauf.

6.2 Verankerung der Gewährleistungsziele in der EU-Datenschutz-Grundverordnung

Mit der EU-Datenschutz-Grundverordnung (DS-GVO) wird das Datenschutzrecht europaweit einheitlich geregelt. Die Verordnung ist am 25.05.2016 in Kraft getreten und gilt gem. Art. 99 Abs. 2 DS-GVO ab dem 25.05.2018 unmittelbar in allen EU Mitgliedstaaten. Für die nationalen Gesetzgeber wurden durch zahlreiche Spezifizierungsklauseln ergänzende Regelungsbe-

fugnisse 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 Verantwortliche und Auftragsverarbeiter dazu, zur Gewährleistung des grundrechtlichen Schutzes der Rechte der Betroffenen sowie gegen unbefugte Zugriffe durch Dritte die dafür angemessenen technischen und organisatorischen Maßnahmen (bspw. in Art. 32, 28 Abs. 3 lit. d DS-GVO) auszuwählen und im Rahmen der Technikgestaltung und datenschutzfreundlicher Voreinstellungen gem. Art. 25 DS-GVO einzusetzen und zu prüfen (Art. 32 Abs. 1 lit. 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 eine Datenschutz-Folgenabschätzung (Art. 35 DS-GVO). Sie enthält eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und fordert im Ergebnis Maßnahmen 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 dazu beitragen, die in Artikel 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 Verantwortliche 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 SDM-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. Unter der Anforderung der „Belastbarkeit“ (Art. 32 Abs. 1 lit. b DS-GVO, engl: „Resilience“) versteht das SDM unter Berücksichtigung des noch unsicheren Interpretationsspielraums die Wahrung der Gewährleistungsziele unter Belastung.

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

6.2.1 Verfügbarkeit

Der Grundsatz der Verfügbarkeit ist in Art. 32 Abs. 1 lit. b und c DS-GVO explizit im Kontext der Sicherheit von Datenverarbeitungen aufgenommen. Es ist zudem in Art. 5 Abs. 1 lit. 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 auch zum Tragen bei den Informations- und Auskunftspflichten (Art. 13 und 15 DS-GVO) gegenüber den Betroffenen. Für die Umsetzung des Rechts auf Datenübertragbarkeit (Art. 20 DS-GVO) ist das Gewährleistungsziel der Verfügbarkeit ebenso Grundvoraussetzung.

6.2.2 Integrität

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

6.2.3 Vertraulichkeit

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

6.2.4 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 lit. c DS-GVO Eingang in die Grundverordnung. Eine darauf folgende Verarbeitung für weitere Zwecke muss mit dem ursprünglichen Zweck kompatibel sein und die Umstände der Verarbeitung berücksichtigen (Art. 6 Abs. 4 DS-GVO). 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 zur Zweckerfüllung nicht erforderlich sind. Über eine Weiterverarbeitung über den ursprünglichen Zweck hinaus, ist der Betroffene zu informieren, der von seinem Widerspruchsrecht Gebrauch machen kann.

Eine typische Maßnahme der Nichtverkettung ist etwa die zweckspezifische Pseudonymisierung. Die Pseudoynmisierung wird beispielsweise in Art. 25 Abs. 1, Art. 32 Abs. 1 lit. a, 40

Abs. 2 lit. d DS-GVO als geeignete Maßnahme zur Umsetzung der Datenschutzgrundsätze genannt.

6.2.5 Transparenz

Der Grundsatz der Transparenz ist in Art. 5 Abs. 1 lit. a DS-GVO festgeschrieben. Er findet sich als tragender Grundsatz des Datenschutzrechts in zahlreichen Regelungen der DS-GVO. Insbesondere die Informations- und Auskunftspflichten gemäß Art. 12 ff. DS-GVO tragen ihm Rechnung.

6.2.6 Intervenierbarkeit

Die Interventionsrechte der Betroffenen ergeben sich explizit aus den Vorschriften zu Berichtigung, Löschung, Widerspruch und zur Einschränkung der Verarbeitung (Art. 16, 17, 18 DS-GVO) sowie der Datenportabilität (Art. 20 DS-GVO). Sie können sich außerdem als Ergebnis einer Interessenabwägung im Rahmen eines gesetzlichen Erlaubnistatbestandes ergeben. Wiederum muss der Verantwortliche gem. Art. 5 Abs. 1 lit. d DS-GVO die Voraussetzung für die Gewährung dieser Rechte, sowohl auf organisatorischer als auch, soweit erforderlich, auf technischer Ebene schaffen.

Tabelle 1: 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, 32 I a), 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 2: 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

In einer Fortschreibung des Handbuchs ist geplant, die Verankerung der Gewährleistungsziele in der EU-Richtlinie für den Datenschutz bei Polizei und Justiz und der in Abstimmung befindlichen ePrivacy-Verordnung der EU zu ergänzen.

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 betroffene 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 Verarbeitungstätigkeiten.

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 `Mitarbeitende.

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 Verarbeitungstätigkeit 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 bei Verarbeitungsverfahren und Komponenten,

- regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung,
- Trennung nach Organisations-/Abteilungsgrenzen,
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten 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 Verarbeitungstätigkeiten insbesondere mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Beschreibungen von Verarbeitungstätigkeiten, Zusammenspiel mit anderen Verarbeitungstätigkeiten,
- Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verarbeitungstätigkeiten,
- Dokumentation der Verträge mit den internen Mitarbeitenden, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen,
- 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 Verarbeitungstätigkeiten 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 Verarbeitungstätigkeiten und deren Komponenten

Als Objekt einer datenschutzgerechten Gestaltung weist die DS-GVO eine „Verarbeitung“ oder „Verarbeitungstätigkeiten“ aus.

Die DS-GVO definiert den Begriff der „Verarbeitung“ in Art. 4 Abs. 2 DS-GVO wie folgt:

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

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

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

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

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

Diese Prüfbilanz bezüglich funktionaler Eigenschaften sowie der getroffenen Schutzmaßnahmen der Verarbeitungstätigkeit muss dann wiederum einer rechtlichen Beurteilung der Rechtskonformität bzw. Ordnungsmäßigkeit insgesamt unterzogen werden können unter

der Fragestellung, ob die richtigen Maßnahmen zweckgemäß ausgewählt und mit der korrekten Wirkintensität betrieben werden.

8.1 Ebenen einer Verarbeitung bzw. Verarbeitungstätigkeit

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

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

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

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

8.2 Zweck

Ob eine Verarbeitung einem legitim gesetzten Zweck folgt und ob der Zweck der Verarbeitung hinreichend bestimmt ist, muss vor der Anwendung des SDM geklärt sein (siehe Abschnitt 10).

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

1. Zusätzlich zur Zweckbestimmung sind die Aspekte der **Zweckabgrenzung** bzw. der **Zwecktrennung** zu betrachten. So sollte festgelegt werden, welche (verwandte) Zwecke nicht mit der Verarbeitungstätigkeit umgesetzt werden sollen. Das erleichtert eine rechtskonforme Abtrennung der Verarbeitungstätigkeiten untereinander sowie insbesondere die Trennung von Datenbeständen, Systemen und Prozessen auf der IT-Ebene.
2. Es ist auch der Aspekt der **Zweckbindung** zu beachten. Die Zweckbindung einer Verarbeitung muss einerseits durch deren geeignete Funktionalität und durch geeignete Auswahl der zu verarbeitenden Produktions- oder Nutzdaten sichergestellt werden (horizontale Gestaltung). Die Zweckbindung einer Verarbeitung muss aber auch durch eine geeignete Ebenen-übergreifende Gestaltung (siehe Abschnitt 8.1) sichergestellt werden (vertikale Gestaltung). So ist es in der Regel nicht vom Zweck abgedeckt und operativ auch nicht notwendig, dass neben den befugten Sachbearbeitern und deren Vorgesetzte auch noch IT-Administratoren, die beispielsweise auf der Ebene einer Datenbank die Zugriffsrechte verwalten oder Kenntnis von den Inhalten der Verarbeitungsdaten nehmen können.

8.2.1 Gewährleistungsziele als Designprinzip

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

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

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

8.3 Komponenten einer Verarbeitung bzw. Verarbeitungstätigkeit

Bei der konkreten Modellierung von Verarbeitungstätigkeiten mit Personenbezug hat es sich bewährt, die folgenden drei Komponenten zu betrachten:

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

Methodisch stehen dabei zunächst die Daten von Personen im Vordergrund, deren Erforderlichkeit der Verarbeitung an der Zweckbestimmung zu bemessen ist. Die konkrete funktionale Gestaltung geschieht auf der Ebene 1, auf der anhand der Daten der Schutzbedarf durch die verantwortliche Stelle festzustellen bzw. festzusetzen ist. Diesen Schutzbedarf erben alle Daten, Systeme und Prozesse, die bei einer konkreten Verarbeitung auf den verschiedenen Ebenen zum Einsatz kommen. Anhand des Referenz-Schutzmaßnahmenkatalogs kann überprüft werden, ob getroffene oder geplante Schutzmaßnahmen dem Schutzbedarf angemessen sind.

Bei diesen drei Kernkomponenten Daten, IT-System und Prozesse spielen u. a. folgende spezielle Eigenschaften noch eine weitere zu beachtende Rolle:

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

Bei den beteiligten Systemen sind die **Schnittstellen** zu betrachten, die eine Fachapplikation mit der Nutzung von IT-Systemen der Ebene 3 sowie insbesondere zu anderen Systemen, die nicht innerhalb der vom Zweck definierten Systemgrenze liegen, aufweist. Der Ausweis der Existenz von Schnittstellen sowie die Dokumentation von deren Eigenschaften sind von entscheidender Bedeutung für die rechtliche Verantwortlichkeit, Beherrschbarkeit und Prüfbarkeit von Datenflüssen.

Für jede Komponente einer Verarbeitungstätigkeit, insbesondere für die manchmal schwierig fassbaren Prozesse über verschiedene Systeme hinweg gilt es, die **Verantwortlichkeit** zu klären. Verantwortlichkeiten werden typischerweise als Rollen in einem umfassenden Rollen- und Berechtigungskonzept formuliert und zugewiesen. Die Verantwortlichkeit eines Prozesseigentümers kann sich auf Hilfsprozesse im Bereich von Technik und organisatorische Regelungen ebenso erstrecken wie im Bereich der Kernprozesse der inhaltlich geprägten Datenverarbeitung oder über alle Prozessebenen eines Verfahrens hinweg im Sinne einer Gesamtverfahrensverantwortlichkeit. Diese Verantwortlichkeit kann auf unterschiedliche Rollen mit jeweils Teilverantwortlichkeiten verteilt werden. **Die Verantwortung für eine Verarbeitung liegt aber letztlich immer beim Verantwortlichen der Organisation, der diese Verarbeitung betreibt**.

9 Risiken und Schutzbedarf

Die DS-GVO gibt dem Verantwortlichen im Erwägungsgrund 76 zwei Stufen zu Bestimmung des Risikos einer personenbezogenen Verarbeitungstätigkeit vor, nämlich „Risiken“ und „hohe Risiken“. Zur Feststellung der Risikostufe ist die Art, der Umfang, die Umstände und die Zwecke der Verarbeitungstätigkeit sowie die spezifischen Eintrittswahrscheinlichkeiten und Schwere der Risiken zu berücksichtigen. Bei der Risikobeurteilung im Rahmen einer Datenschutzfolgenabschätzung sind zusätzliche die Ursache der Risiken detaillierter zu ermitteln. Es ist Aufgabe des Verantwortlichen, diese Risiken zu identifizieren, zu analysieren und einzustufen und Maßnahmen zu deren Eindämmung zu treffen. Eine erste Risikobewertung muss bereits vor der Anwendung des SDM erfolgen. Das SDM ist dabei Teil eines iterativen Prozesses der rechtlichen Bewertung, der Risikoeinstufung und der Auswahl und Umsetzung von technischen und organisatorischen Maßnahmen (siehe Abschnitt 2).

Zur Gestaltung der Funktionalität einer Verarbeitung und zur Bestimmung von Schutzmaßnahmen ist es wichtig, einerseits den **Aspekt des Grundrechteeingriffs und dessen Intensität**, der mit jeder personenbezogenen Datenverarbeitung zwangsläufig einhergeht, und andererseits den **Aspekt der sicheren Gestaltung eines Verfahrens im Sinne der IT-Sicherheit** zu unterscheiden. Risiken eines Grundrechtseingriffs und Risiken der IT-Sicherheit erfordern unterschiedliche Maßnahmen zu deren Eindämmung.

Aus dem Aspekt des Grundrechtseingriffs und dessen Intensität resultieren die spezifischen Maßnahmen des Datenschutzes, die darauf abzielen, die Intensität eines Grundrechteingriffs auf das geringstmögliche Maß zu verringern. Dies erfordert im ersten (juristischen) Schritt abzuwägen, ob der Grundrechtseingriff erforderlich und die Eingriffsintensität akzeptabel sind. Im Ergebnis sind die Funktionen einer Verarbeitung auszugestalten. Dabei ist zu berücksichtigen, dass das für den Datenschutz wesentliche Risiko für Betroffene darin besteht, dass eine Verarbeitungstätigkeit nicht den Anforderungen der DS-GVO genügt. Um dieses Risiko angemessen bewerten zu können, ist immer der Bezug zwischen den Verarbeitungsgrundsätzen der DS-GVO (Art. 5) und den Gewährleistungszielen des SDM herzustellen.

Aus dem Aspekt der sicheren Gestaltung eines Verfahrens im Sinne der IT-Sicherheit erfolgt die Ausgestaltung der IT-Sicherheit mit dem Bezug zu dem Betroffenen zunächst eher technisch orientiert. Aber auch die Maßnahmen der IT-Sicherheit müssen datenschutzgerecht bzw. grundrechtskonform ausgestaltet werden und einer rechtlichen Beurteilung unterzogen werden.

Um die beiden Risiken in Eigenschaften von Schutzfunktionen zu transformieren, nutzt das SDM in Anlehnung an die BSI-Grundschutzmethodik die drei Schutzbedarfsklassen „normaler Schutzbedarf“, „hoher Schutzbedarf“ und „sehr hoher Schutzbedarf“ mit folgender Zuordnungsfunktion: Je größer die Risiken, desto höher ist der Gewährleistungsbedarf, dass das Verfahren gesichert funktionale, datenschutzgerechte Eigenschaften (vgl. Art. 5 DS-GVO)

und angemessen wirksame Schutzmaßnahmen zur Abwehr von Schadens- und Verlustereignissen aufweist (vgl. Art. 32 DS-GVO in Verbindung mit EG 75).

Die Schutzbedarfseinstufung nach dem SDM folgt insofern der zuvor durch den Verantwortlichen festgesetzten Risikostufe. Wenn ein Risiko besteht, entspricht dies in der Regel einem „normalen Schutzbedarf". Folgerichtig müssen die Maßnahmen zur Umsetzung der Anforderungen gem. Art. 5 DS-GVO den „normalen Schutzbedarf“ umsetzen. Ein „hohes Risiko“ entspricht einem „hohen Schutzbedarf“ und führt zu Maßnahmen mit entsprechend höheren Anforderungen an deren Wirkintensität oder erfordert sogar zusätzliche Maßnahmen. Für „sehr hohen Schutzbedarf“, der wiederum aus einem „sehr hohen Risiko“ folgte, weist das SDM keine Standard-Referenzmaßnahmen aus. Hier sind zusätzlich zu den Maßnahmen des hohen Schutzbedarfs weitere, speziell auf die Verarbeitung abgestimmte Schutzmaßnahmen auszuwählen und umzusetzen.

Zu beachten ist, dass das Risiko immer zuerst ermittelt werden muss. Ein hohes Risiko nach DS-GVO zieht einen hohen Schutzbedarf nach BSI-Grundschutz nach sich. Dies bedeutet insbesondere bei der Bewertung von besonderen Arten personenbezogener Daten, dass eine hohe Eingriffstiefe nicht immer (aber häufiger) zu einem hohen Risiko und damit zu einem hohen Schutzbedarf führt.

Hoher Schutzbedarf führt nicht zwangsläufig dazu, dass eine Vielzahl zusätzlicher Maßnahmen getroffen werden müssen. Vielmehr ist es zunächst sinnvoll, die Wirkung einer Maßnahme zu erhöhen (bspw. die Nutzung eines längeren kryptographischen Schlüssels). Zudem kann dafür gesorgt werden, dass die spezifikationsgerechte Ausführung einer Maßnahme dadurch in einem noch mal erhöhten Maße zuverlässig erfolgt, indem die Robustheit dieser Maßnahme, durch zusätzliche Vorkehrungen etwa im organisatorischen Bereich, erhöht wird. Ganz wesentlich gilt jedoch die Regel, dass Schutzmaßnahmen für hohen Schutzbedarf selbst den Anforderungen der Gewährleistungsziele genügen müssen. So müssen bspw. bestimmte Ereignisse nicht nur protokolliert werden, sondern bei der Speicherung der Protokolldaten sind Schutzmaßnahmen zu treffen, die alle Gewährleistungsziele sicherstellen. Protokolle müssen bspw. gesichert verfügbar, integritätsgeschützt und nochmals vor unbefugtem Zugriff gesichert sein sowie und einer gesonderten Zweckbindung unterliegen. Dies kann die o. g. höhere Wirkintensität vorhandener Maßnahmen oder zusätzliche Maßnahmen wie die Nutzung eines dedizierten Protokollservers erfordern.

Das SDM enthält einen Katalog von Einzelmaßnahmen bezogen auf normalen oder hohen Schutzbedarf, die in verschiedenen Bausteinen systematisiert wurden. Der Verantwortlich kann diese Maßnahmen als Referenzmaßnahmen nutzen, um die oben beschriebenen Risiken einzudämmen. Er kann aber auch andere Maßnahmen als die vom SDM ausgewiesenen Maßnahmen umsetzen und die Wirkintensität der Maßnahmen bei hohem Schutzbedarf anders erhöhen, als vom SDM empfohlen wird. In diesem Fall sollte der Verantwortliche aber in der Lage sein nachzuweisen, dass die anderen oder modifizierten Maßnahmen einen mindestens gleichwertigen Schutz bieten wie die Referenzmaßnahmen des SDM.

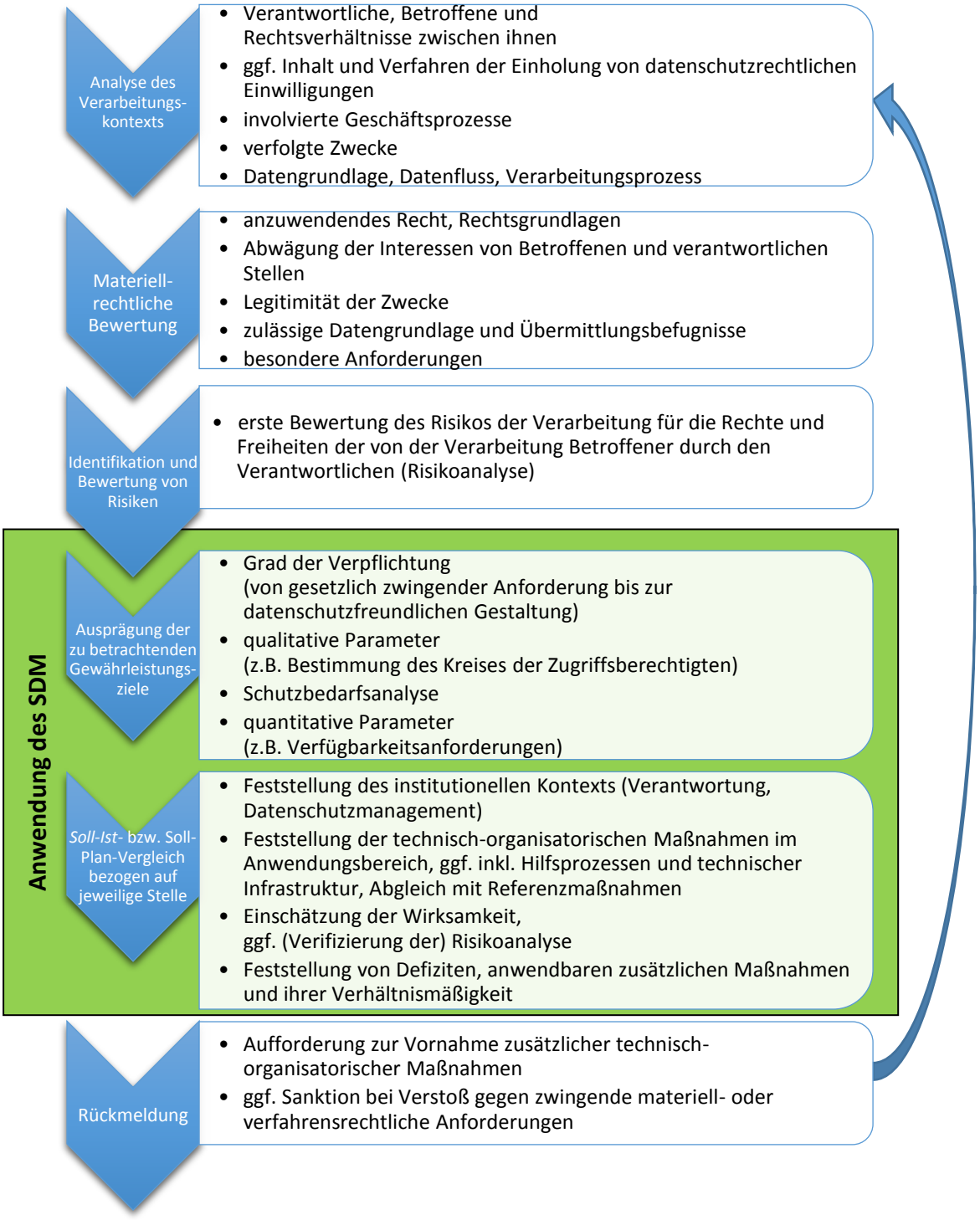
Die Methodik des IT-Grundschutz des BSI nutzt ebenfalls das Konzept der Schutzbedarfseinstufungen, um die Wirkung von Schutzmaßnahmen angemessen skalieren zu können. Wegen der unterschiedlichen Zielrichtungen von IT-Sicherheit durch die Verwendung des IT-Grundschutz des BSI und dem operativen Datenschutz durch die Nutzung des SDM kann nicht ausgeschlossen werden, dass die Schutzbedarfsfeststellungen nach Grundschutz und nach SDM für dieselbe Verarbeitung unterschiedlich ausfallen.

Als Beispiel für einen solchen Konflikt kann die Protokollierung von Nutzeraktionen herangezogen werden. Aus Sicht der IT-Sicherheit liegt es nahe, sämtliche Aktivitäten zu erfassen; aus Sicht des Datenschutzes sind Vollprotokollierungen nur in wenigen Fällen akzeptabel. Die Gründe, die eine Vollprotokollierung rechtfertigen, müssten nachvollziehbar dokumentiert werden. Allerdings gelten auch beim IT-Grundschutz personenbezogene Daten als besonders schutzbedürftig. Da die Informationssicherheit auch von grundrechtlichen Erwägungen geleitet sein muss, wird in der Regel eine Schutzbedarfsbetrachtung nach IT-Grundschutz zu gleichen Ergebnissen kommen wie die Schutzbedarfsbetrachtung nach SDM. Kommt es dennoch zu unterschiedlichen Einstufungen, muss bei einer datenschutzrechtlichen Prüfung die Schutzbedarfsfeststellung nach den datenschutzrechtlichen Prinzipien des SDM den Vorrang haben.

Die Grundschutzmethodik kennt zudem die Regelung der kumulativen Effekte, wonach bspw. für Daten mit normalem Schutzbedarf durch den bloßen Umstand der Massenverarbeitung hoher Schutzbedarf besteht. Solche Überlegungen müssen bereits in die Überlegungen zur Einstufung des Risikos durch den Verantwortlichen einfließen. Die DS-GVO erfasst diese Überlegung in Art. 34 mit dem Hinweis u. a. auf den Umfang einer Verarbeitung.

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 Beratungsersuche fokussieren in aller Regel auf spezifische Aspekte einer Verarbeitungstätigkeit 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 (siehe auch Abschnitt 2).

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 basie-

ren 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 oder Auftragsverarbeiter 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 Erfül-

lung 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 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.

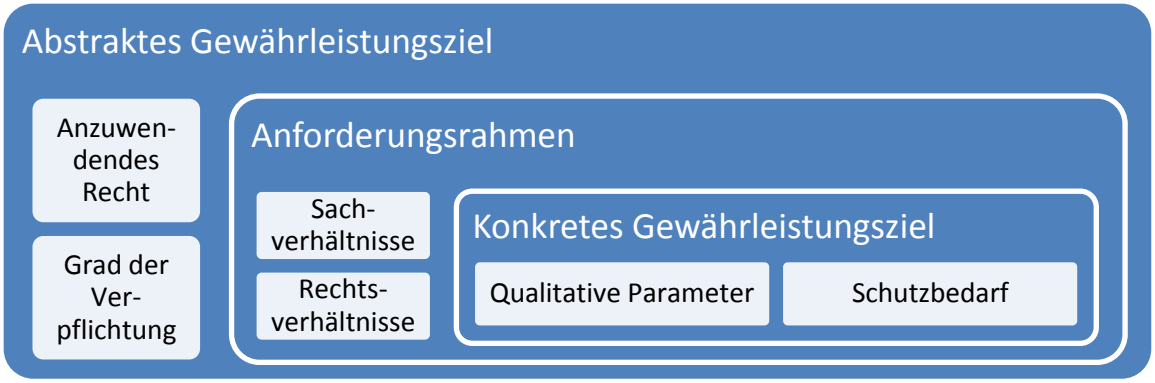


Abbildung 1: Ausprägung der Gewährleistungsziele

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 Dokumentation der Verarbeitung nach Art. 30 DS-GVO, 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 Risikobestimmung samt nachgelagerter Schutzbedarfsanalyse erfolgen bzw. die Schutzbedarfsanalyse des Verantwortlichen 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 des Verantwortlichen. 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 Beteiligten 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 verarbeiten.

10.3 Der Soll-Ist-Vergleich

Der Kern der Anwendung des SDM 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 (dort insbesondere von den Datenschutzbeauftragten) bei der Planung und beim Betrieb der 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.

Der Maßnahmenkatalog ist in einzelne, verabeitungsspezifische Bausteine gegliedert. Jeder Baustein enthält Baustein spezifische Maßnahmen auf der Ebene der Daten, IT-Systeme und Prozesse. Dieser Katalog von Bausteinen befindet sich in der Entwicklungs- und Abstimmungsphase und wird ständig weiterentwickelt.

Im Rahmen Erprobung des SDM werden die einzelnen Bausteine des Katalogs zunächst von einzelnen Aufsichtsbehörden veröffentlicht und getestet, um ihre Praxistauglichkeit erproben und nachweisen zu können. Wenn der Nachweis der Praxistauglichkeit dieser Bausteine erbracht ist, werden sie als verbindliche SDM-Bausteine vom AK Technik veröffentlicht. Auf diese Weise wird die Maßnahmenkatalog

13 Stichwortverzeichnis

14 Die vorgenommenen Änderungen von SDM-V1.0 auf SDM-V1.1

(Stand: 23. März 2018)

Die folgenden Änderungen betreffen den gesamten Text:

- Das SDM referenziert in der vorliegenden Version ausschließlich auf die DS-GVO; die Bezüge zum BDSG und zu den Landesdatenschutzgesetzen wurden herausgenommen. Möglicherweise müssen Bezüge zum BDSGneu und zu den novellierten Landesdatenschutzgesetzen neu hergestellt werden. Diese Bezüge herzustellen bleibt einer weiteren Fortschreibung des SDM vorbehalten.

- Der Begriff "Verfahren" wurde an vielen Stellen ersetzt durch den in der DS-GVO verwendeten Begriff der "Verarbeitung" oder der "Verarbeitungstätigkeit", ebenso wurde der Begriff "Grundrecht" oder "grundrechtlich" auf die DS-GVO-Formel "Rechte und Freiheiten von Personen" umgestellt.

- Es wurde darauf geachtet, dass das SDM insgesamt auch international anschlussfähig ist, wobei Bezüge zu Urteilen des BVerfG erhalten blieben.

- Ergänzung dieses Kapitels, das die Änderungen zur vorigen Version auflistet.

Wesentliche Änderungen in den einzelnen Kapiteln:

"Kap. 1 Einleitung" wurde vollständig überarbeitet; neu ist der ausschließliche Bezug zur DS-GVO.

"Kap. 2 Der Zweck des Standard-Datenschutzmodells" wurde vollständig überarbeitet; herausgestellt wurde deutlicher als bislang, dass vor dem Einsatz des SDM zur Auswahl und Konfiguration von Schutzmaßahmen die rechtlichen Abwägungs- und Erforderlichkeits-Prozesse sowie eine erste Risikoanalyse durchgeführt sein müssen.

"Kap. 5.5 Weitere abgeleitete Gewährleistungsziele" wurde ersatzlos gelöscht.

"Kap 6.2 Verankerung der Gewährleistungsziele im BDSG" und "Kap. 6.3 Verankerung der Gewährleistungsziele in den Landesdatenschutzgesetzen" und jeweils alle Unterkapitel wurden gelöscht. Ergänzt wurde in "Kap. 6.2 Verankerung der Gewährleistungsziele in der EU-Datenschutz-Grundverordnung" der Passus: "In einer Fortschreibung des Handbuchs ist geplant, die Verankerung der Gewährleistungsziele in der EU-Richtlinie für den Datenschutz bei Polizei und Justiz und der in Abstimmung befindlichen ePrivacy-Verordnung der EU zu ergänzen."

"Kap. 8 Die Verfahrenskomponenten" wurde vollständig überarbeitet. Zum einen musste auf den Begriff der "Verarbeitung" bzw. "Verarbeitungstätigkeit" umgestellt werden, zum anderen hat sich in der Praxis gezeigt, das Bedarf daran besteht, die verschiedenen Ebenen der Vorstellungen zum Begriff "Verarbeitung" zu klären und welche Aspekte bei einer Zweck- oder Zweckebestimmung und Zweckbindung bedacht werden sollten.

"Kap. 9 Der Schutzbedarf" wurde vollständig überarbeitet. Die DS-GVO enthält bereits ein gewisses Maß an methodischer Anleitung zur Risikoermittlung, weshalb eine Anleitung zur methodischen Ermittlung von Risiken bzw. des Schutzbedarfs entbehrlich wurde.

Das Standard-Datenschutzmodell

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

V.1.1 – Erprobungsfassung