Das Standard-Datenschutzmodell

Konzept zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele

V.0.9 zum Umlauf im Anschluss an die 65. Sitzung des AK Technik am 8. und 9. September 2015 in Schwerin zwecks Entscheidung über Vorlage auf der 90. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 30. September und 1. Oktober 2015 in Darmstadt

Inhalt

1 Einleitung ... 3
2 Der Zweck des Standard-Datenschutzmodells ... 4
3 Der Anwendungsbereich des Standard-Datenschutzmodells ... 5
4 Die Struktur des Standard-Datenschutzmodells ... 6
5 Die Gewährleistungsziele ... 6
5.1 Der Begriff „Gewährleistungsziel“ ... 6
5.2 Die zentralen datenschutzrechtlichen Anforderungen ... 6
5.3 Das grundlegende Gewährleistungsziel Datensparsamkeit ... 7
5.4 Die elementaren Gewährleistungsziele ... 9
5.5 Weitere abgeleitete Gewährleistungsziele ... 11
6 Der Bezug der Gewährleistungsziele zum bestehenden Datenschutzrecht ... 13
6.1 Gewährleistungsziele in der Rechtsprechung des Bundesverfassungsgerichts ... 13
6.2 Verankerung der Gewährleistungsziele im BDSG ... 14
6.2.1 Gewährleistungsziele als Prüfungsmaßstab ... 14
Datensparsamkeit ... 16
Verfügbarkeit ... 16
Integrität ... 16
Vertraulichkeit ... 16
Nichtverkettbarkeit ... 16
Transparenz ... 17
Intervenierbarkeit ... 17

6.2.2 Verankerung der Anwendbarkeit der Gewährleistungsziele auf personenbezogene Verfahren 19
6.3 Verankerung der Gewährleistungsziele in den Landesdatenschutzgesetzen 20
6.4 Verankerung der Gewährleistungsziele in der EU-Datenschutzrichtlinie 22
7 Die generischen Maßnahmen zur Umsetzung der Gewährleistungsziele 23
7.1 Gewährleistungsziel Datensparsamkeit 23
7.2 Gewährleistungsziel Verfügbarkeit 23
7.3 Gewährleistungsziel Integrität 24
7.4 Gewährleistungsziel Vertraulichkeit 24
7.5 Gewährleistungsziel Nichtverkettbarkeit 24
7.6 Gewährleistungsziel Transparenz 25
7.7 Gewährleistungsziel Intervenierbarkeit 25
8 Die Verfahrenskomponenten 27
9 Der Schutzbedarf 29
9.1 Die Schutzbedarfsabstufungen 29
9.2 Objektbereiche 29
9.3 Definition der Schutzbedarfskategorien 29
9.4 Schadensszenarien für Betroffene 29
10 Prüfen und Beraten auf der Grundlage des Standard-Datenschutzmodells 32
10.1 Vorbereitung 33
10.2 Spezifizierung der Gewährleistungsziele 35
10.3 Der Soll-Ist-Vergleich 37
11 Das Betriebskonzept zum Standard-Datenschutzmodell 38
11.1 Einleitung 38
11.2 Auftraggeber, Projektleitung, Anwender 38
12 Schutzmaßnahmen-Referenzkatalog 40

1 Einleitung

Am 24. September 2010 hat der IT-Planungsrat die Nationale E-Government Strategie (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. Diese Strategie ist die Basis für die **Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik**. Die NEGS strebt die gemeinsame strategische Ausrichtung von Bund, Ländern und Kommunen in der Weiterentwicklung von E-Government an und möchte das Handeln der Beteiligten koordinieren, um Interoperabilität und Wirtschaftlichkeit zu sichern. Sie zielt dabei auch auf die Gewährleistung von Datenschutz und Datensicherheit ab, damit die Bürger dem E-Government vertrauen, es akzeptieren und auch intensiv nutzen.

Die Datenschutzbehörden müssen vor diesem Hintergrund in zunehmendem Maße zusammen arbeiten, mit bundesweit einheitlichen Beratungs- und Prüfkonzepten die modernen Verfahren zur automatisierten Verarbeitung personenbezogener Daten begleiten und auf eine datenschutzkonforme Umsetzung der NEGS hinwirken. Einheitliche Prüf- und Beratungskonzepte können dabei zu einem abgestimmten, transparenten und nachvollziehbaren System der datenschutzrechtlichen Bewertung führen. Dies betrifft insbesondere länderübergreifende E-Government-Verfahren etwa im Meldewesen, im Personenstandswesen, im Sozialwesen oder im Bereich der Steuerdatenverarbeitung.

Auch für die Datenschutzaufsicht im Bereich der privaten Wirtschaft wird ein solches abgestimmtes Handeln immer wichtiger. Die Verarbeitung personenbezogener Daten im Bereich des E-Commerce ist schon lange nicht mehr auf den Bereich einzelner Bundesländer und damit auf den Zuständigkeitsbereich einzelner Datenschutzaufsichtsbehörde beschränkt, sondern überschreitet inzwischen die Grenzen Deutschlands und die der Europäischen Union. Der Entwurf der Europäischen Datenschutz-Grundverordnung sieht daher ein Kohärenzverfahren vor, das die unabhängigen Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet. Auch dieses Verfahren erfordert das oben erwähnte abgestimmte, transparente und nachvollziehbare System zur datenschutzrechtlichen Bewertung der Verarbeitung personenbezogener Daten.

Das hier beschriebene Standard-Datenschutzmodell soll dazu einen wesentlichen Beitrag sowohl im öffentlich-rechtlichen als auch im privat-rechtlichen Bereich leisten, indem es einen systematischen und nachvollziehbaren Vergleich ermöglicht zwischen Sollvorgaben, die sich aus Normen, Verträgen, Einwilligungserklärungen und Organisationsregeln ableiten, einerseits und ihrer Umsetzung sowohl auf organisatorischer wie auch informationstechnischer Ebene in IT-Verfahren und -Systemen ermöglicht.

2 Der Zweck des Standard-Datenschutzmodells

Die Verarbeitung personenbezogener Daten mit Hilfe informationstechnischer Verfahren ist datenschutzrechtlich danach zu beurteilen, ob sie auf einer ausreichenden Rechtsgrundlage erfolgt. Es gilt das Verbot mit Erlaubnisvorbehalt des § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) bzw. der entsprechenden Normen der Landesdatenschutzgesetze. Zudem ist zu prüfen, ob die Daten durch eine angemessene Auswahl technischer und organisatorischer Maßnahmen so verarbeitet werden, dass die Rechte der Betroffenen gewahrt bleiben.

Das hier beschriebene Standard-Datenschutzmodell soll diese Maßnahmen auf der Basis von Schutzzielen systematisieren. Damit dient das Modell einerseits den für die Verarbeitung verantwortlichen Stellen, erforderliche Maßnahmen systematisch zu planen und umzusetzen und fördert somit die datenschutzgerechte Ausgestaltung und Organisation von informationstechnischen Verfahren und Applikationen. Andererseits bietet das Modell den Datenschutzbehörden eine Möglichkeit, mit einer einheitlichen Systematik zu einem transparenten, nachvollziehbaren, belastbaren Gesamturteil über ein Verfahren und dessen Komponenten zu gelangen.

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

3 Der Anwendungsbereich des Standard-Datenschutzmodells

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

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

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

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

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

4 Die Struktur des Standard-Datenschutzmodells

Das Standard-Datenschutzmodell

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

5 Die Gewährleistungsziele

5.1 Der Begriff „Gewährleistungsziel“

Das Standard-Datenschutzmodell verwendet für die Beschreibung von bestimmten aus dem Datenschutzrecht resultierenden Kategorien von Anforderungen den Begriff „Gewährleistungsziel“. Der Begriff „Schutzziel“ wird bewusst nicht benutzt, weil es ein vorherrschend enges Vorverständnis von Schutzzielen gibt, das insbesondere von der IT-Sicherheit schon über Jahrzehnte geprägt wurde. Wenn bspw. nachfolgend vom "Schutz der Integrität" die Rede ist, dann soll dieser nicht nur die Bildung und den Vergleich von Hashwerten für Daten betreffen. Vielmehr soll der Schutz der Integrität das gesamte Verfahren betreffen, das die Komponenten Daten, Systeme und Prozesse umfasst.

Zudem ist der Begriff „Gewährleistungsziel“ besonders gut geeignet, um den Bezug zum Urteil des Bundesverfassungsgerichts von 2008 herzustellen. Das Bundesverfassungsgericht hatte seinerzeit das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abgeleitet (siehe auch Punkt 6.1).

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

5.2 Die zentralen datenschutzrechtlichen Anforderungen

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

- die Zweckbindung einer Datenverarbeitung mit Personenbezug,

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

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

5.3 Das grundlegende Gewährleistungsziel Datensparsamkeit

Allen Gewährleistungszielen ist gemein, dass sie bestimmen, welche Eigenschaften und Parameter von im Vorhinein als zulässig bestimmten Verarbeitungsvorgängen und Begleitprozessen zu wahren sind. Die Maßnahmen, die sich aus ihnen ableiten, halten den Verarbeitungsfluss gewissermaßen mit Ufern und Deichen in vorbestimmten Bahnen. Dabei gilt: Je dünner der Fluss, desto geringer die Gefahren, desto niedriger dürfen die Deiche im weiteren Verlauf sein. Daher fordert der Gesetzgeber, den Datenstrom selbst in seinem Umfang zu zähmen, ihn zu reduzieren, an der Quelle und jeder Verzweigung, im Vorhinein und – immer wichtiger im Zeitalter der mit dem Stichwort *Big Data* verknüpften explorativen Datenverarbeitung – im Zuge der Verarbeitung selbst. Diese grundlegende Anforderung erfasst das Gewährleistungsziel der Datensparsamkeit, dessen Umsetzung daher einen durchgreifenden Einfluss auf Umfang und Intensität des durch die anderen Gewährleistungsziele bestimmten Schutzprogramms hat.

Datensparsamkeit konkretisiert und operationalisiert im Verarbeitungsprozess den Grundsatz der Erforderlichkeit, der von diesem Prozess insgesamt wie auch von jedem seiner Schritte verlangt, nicht mehr personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen, als für das Erreichen des Verarbeitungszwecks erforderlich ist. Datensparsamkeit ist als proaktives Element datenschutzfreundlicher Technikgestaltung zu berücksichtigen: beginnend beim Design der Informationstechnik durch den Hersteller, über ihre Konfiguration und Anpassung an die Betriebsbedingungen, bis zu ihrem Einsatz in den Kernprozessen des Verfahrens wie auch in den unterstützenden Prozessen zum Beispiel bei der Wartung der verwendeten Systeme, von der Erhebung der personenbezogenen Daten über ihre Verarbeitung und Nutzung bis zur Löschung oder vollständigen Anonymisierung, über den vollständigen Lebenszyklus der Daten hinweg.

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

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

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

Das Gewährleistungsziel der Datensparsamkeit 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. Vorgehensweisen, bei denen die Daten bei der verantwortlichen Stelle verbleiben und nicht mit Dritten geteilt werden, sind denjenigen vorzuziehen, bei denen Daten an verschiedene Stellen weitergegeben werden. Sollten personenbezogene Daten jedoch so zwischen zwei Stellen aufgeteilt werden, dass es gemeinsamen Handelns bedarf, um sie zu rekonstituieren, so ist dies gegenüber einer zentralisierten Datenhaltung zu bevorzugen.

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

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

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

5.4 Die elementaren Gewährleistungsziele

Gewährleistungsziele spielen seit Ende der 1980er Jahre 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 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, was u. a. voraussetzt, dass die Methoden mit den vorliegenden Datenformaten umgehen können. Die Verfügbarkeit schließt neben der Auffindbarkeit der Daten und der Fähigkeit der verwendeten Systeme, sie angemessen darzustellen, auch die Begreifbarkeit der Daten (ihre semantische Erfassbarkeit) ein.

(2) Das Gewährleistungsziel *Integrität* bezeichnet die Anforderung, dass informationstechnische Prozesse und Systeme die Spezifikationen kontinuierlich einhalten, die zur Ausübung ihrer zweckbestimmten Funktionen für sie festgelegt wurden, und die mit ihnen zu verarbeitenden Daten unversehrt, vollständig und aktuell bleiben. Etwaige Nebenwirkungen müssen ausgeschlossen oder aber berücksichtigt und bearbeitet sein. Dieses Gewährleistungsziel enthält die Anforderung, dass zwischen dem Sollen und dem Sein eine hinreichende Deckung besteht, sowohl bei technischen Details wie auch im großen Zusammenhang des Verfahrens und dessen Zwecksetzung insgesamt.

(3) Das Gewährleistungsziel *Vertraulichkeit* bezeichnet die Anforderung, dass keine Person personenbezogene Daten unbefugt zur Kenntnis nimmt. Eine Kenntnisnahme besteht oft bereits darin, dass Betroffene durch Einsicht in ein System identifiziert werden, da der Kontext, in dem die Speicherung stattfindet, bereits weitergehende Schlussfolgerungen über die Betroffenen erlaubt. Unbefugte sind nicht nur Dritte außerhalb der verantwortlichen Stelle, mögen sie mit oder ohne kriminelle Absicht handeln, sondern auch Beschäftigte von technischen Dienstleistern, die zur Erbringung der Dienstleistung keinen Zugriff zu personenbezogenen Daten benötigen, oder Personen in Organisationseinheiten, die keinerlei inhaltlichen Bezug zu einem Verfahren oder zu der oder dem jeweiligen Betroffenen haben.

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

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

Diese Datenschutz-Gewährleistungsziele, die die oben aufgelisteten zentralen datenschutzrechtlichen Anforderungen in einer operationalisierbaren Form wiedergeben sollen und deshalb spezifisch auf den Schutzbedarf von Betroffenen ausgerichtet sind, lauten:

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

(4) Das Gewährleistungsziel Nichtverkettbarkeit bezeichnet die Anforderung, 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 sind erfahrungsgemäß die Begehrlichkeiten, die Daten zweckentfremdet zu nutzen. Rechtlich zulässig sind jedoch derartige Nachnutzungen nur unter eng definierten Umständen. Das Datenschutzrecht fordert darüber hinaus, dass eine Verarbeitung nach Zwecken getrennt ermöglicht werden muss (Funktionstrennung) bzw. dass die Daten je nach Verarbeitungszweck voneinander getrennt gespeichert werden (Datentrennung) werden. Ggf. muss der Datenbestand durch Duplizie-

rung und Reduzierung auf den für den neuen Zweck erforderlichen Umfang angepasst werden.

Wie für die klassischen, so gilt auch für die datenschutzspezifischen Gewährleistungsziele, dass die Ausprägung, in der sie zu erreichen sind, vom jeweils anwendbaren Datenschutzrecht abhängt. So erstreckt sich im nichtöffentlichen Bereich die Transparenz nicht notwendig auf einzelne Nutzungsvorgänge innerhalb der verantwortlichen Stelle, soweit sie nicht mit einer Veränderung der Daten einhergehen.

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

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

5.5 Weitere abgeleitete Gewährleistungsziele

Andere, bisher nicht aufgeführte Gewährleistungsziele, deren Sicherung von Landesdatenschutzgesetzen oder bereichsspezifischen Datenschutznormen gefordert wird, lassen sich aus den oben genannten elementaren Gewährleistungszielen ableiten. Folgende abgeleitete Gewährleistungsziele sind insbesondere zu nennen:

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

Je nach Art des Ursprungs sind unterschiedliche Angaben festzuhalten und die Verknüpfung der Daten mit diesen Angaben zu schützen: Im Falle von Erhebungen bei den Betroffenen selbst schließen diese Angaben den Erhebungsprozess, den Zeitpunkt seines Ablaufs und ggf. die Identität der erhebenden Personen ein; im Falle der Entgegennahme von Übermittlungen oder dem Abruf aus Datenbeständen Dritter sind dies Zeitpunkt, Anlass und Zweck von Übermittlung bzw. Abruf, sowie die Datenquelle; im Falle einer Zweck ändernden Übernah-

me eines Datenbestandes Bezeichnung und Revisionsstand des Quelldatenbestandes sowie ein Verweis auf dessen Dokumentation.

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

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

6 Der Bezug der Gewährleistungsziele zum bestehenden Datenschutzrecht

Normen lassen sich nicht ohne weiteres technisch operationalisieren. In der datenschutzrechtlichen Prüfung müssen Juristen und Informatiker deshalb eine gemeinsame Sprache finden, um sicherzugehen, dass die rechtlichen Anforderungen auch tatsächlich technisch umgesetzt werden. Hierbei werden sie durch die Gewährleistungsziele unterstützt, denn die datenschutzrechtlichen Anforderungen können entsprechend ihres Gehalts, ihrer beabsichtigten Wirkung und Zielrichtung den einzelnen Gewährleistungszielen zugeordnet und auf diese Weise strukturiert gebündelt werden. Die technische Gestaltung von Systemen richtet sich an diesen Zielen aus, 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/Nichtverkettbarkeit, Erforderlichkeit, Transparenz und Intervenierbarkeit sowie der Sicherheit der Datenverarbeitung ableitbar, die flankiert durch die daran ausgerichtete Verfahrensgestaltungen, das Recht auf informationelle Selbstbestimmung schützen bzw. zu dessen Entfaltung beitragen sollen.

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

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

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

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

6.2 Verankerung der Gewährleistungsziele im BDSG

6.2.1 Gewährleistungsziele als Prüfungsmaßstab

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

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

§ 9 Satz 1 BDSG legt fest, dass die datenschutzrechtlichen Anforderungen durch technisch-organisatorische Maßnahmen zu operationalisieren sind. Zur Ermittlung, welche Maßnahmen zur Einhaltung der Gesetze erforderlich sind, dienen die Gewährleistungsziele, die auf der einen Seite die datenschutzrechtlichen Anforderungen bündeln und strukturieren und auf der anderen Seite durch technische Umsetzung erreicht werden können.

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

Die datenschutzrechtlichen Vorschriften können ihrem Gehalt und ihrer Zielrichtung entsprechend den Gewährleistungszielen zugeordnet werden (sog. „Mapping"). Diese Strukturierung ermöglicht die Operationalisierung der datenschutzrechtlichen Anforderungen in prüffähiger und standardisierter Form. Auf diese Weise wird die verantwortliche Stelle darüber hinaus unterstützt, den Nachweis darüber zu führen, dass die erforderlichen Maßnahmen zur Vermeidung von Rechtsverstößen auch tatsächlich ergriffen wurden.

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

Datensparsamkeit

Das Gebot der Datensparsamkeit ist in § 3a BDSG geregelt und ergibt sich aus dem allgemeinen Grundsatz der Erforderlichkeit, der als zentrale Voraussetzung in den Erlaubnistatbeständen zum Ausdruck kommt (z. B. § 28 BDSG). Die Regelung des § 3a Satz 1 BDSG stellt klar, dass der Grundsatz bereits bei bei der Auswahl und Gestaltung von Datenverarbeitungssystemen anzuwenden ist.

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

Verfügbarkeit

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

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

Integrität

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

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

Vertraulichkeit

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

Nichtverkettbarkeit

Die Verpflichtung, Daten **nur für den Zweck** zu verarbeiten, zu dem sie erhoben wurden, ist insbesondere den einzelnen Verarbeitungsbefugnissen zu entnehmen, die die Geschäftszwecke, die Forschungszwecke etc. zum Maßstab machen. Bei der Datenverarbeitung auf der

Grundlage der Einwilligung ergibt sich aus § 4a Abs. 1 Satz 2 BDSG, dass auf den vorgesehenen Zweck hinzuweisen ist. Der Zweck ist demnach festzulegen und die Einwilligung erstreckt sich nur auf die Verarbeitung zu diesem Zweck.

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

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

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

Transparenz

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

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

Die Kontroll- bzw. Aufsichtsbehörden haben Auskunfts- und Einsichtsrechte nach §§ 24 bzw. 38 BDSG.

Zudem sind Verfahrensverzeichnisse zu erstellen, die von **jedermann** gemäß § 38 Abs. 2 BDSG bzw. § 4g Absatz 2 Satz 2 BDSG eingesehen werden können.

Intervenierbarkeit

Die Interventionsrechte der Betroffenen ergeben sich explizit aus den Vorschriften zu Benachrichtigung, Auskunft, Berichtigung, Sperrung, Löschung und Widerspruch. Sie können sich außerdem als Ergebnis einer Interessenabwägung im Rahmen eines gesetzlichen Erlaubnistatbestandes ergeben. Wiederum müssen die verantwortlichen Stellen gem. Satz 1 der Anlage zu § 9 BDSG die Voraussetzung für die Gewährung dieser Rechte, sowohl auf organisatorischer als auch, soweit erforderlich, auf technischer Ebene schaffen.

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

	Datensparsamkeit	**Verfügbarkeit**	**Integrität**	**Vertraulichkeit**	**Nichtverkettbarkeit**	**Transparenz**	**Intervenierbarkeit**
§ 3a	§ 3a						
§ 4	§ 4 Abs. 2 Nr. 2a				§ 4 Abs. 3 Nr. 2	§ 4 Abs. 3	§ 4 Abs. 1
§§ 4a, 4b, 4c, 4d, 4e, 4f, 4g					§ 4a Abs. 1 Satz 2 § 4b Abs. 6 § 4c Abs. 1 Satz 2 § 4e Nr. 4	§ 4a Abs. 1 Satz 2-4, Abs. 2Satz 2, Abs. 3 § 4d Abs. 1 Satz 1, § 4d Abs. 5 § 4e § 4g Abs. 2	§ 4c Abs. 1 Satz 1 Nr. 1
§ 5				§ 5 Satz 1, Satz 2, Satz 3			
§§ 6, 6a, 6b, 6c	§ 6b Abs. 1, Abs. 3, Abs. 5				§ 6 Abs. 3 § 6b Abs. 1, § 6b Abs. 3 Satz 3, § 6b Abs. 5	§ 6 Abs. 1, Abs. 2 Sätze 1-3 § 6a Abs. 2 Nr. 2 § 6b Abs. 2, Abs. 3,§ 6b Abs. 4 § 6c Abs. 1, Abs. 3	§ 6 Abs. 1, § 6 Abs. 2 Satz 1 § 6a Abs. 1 Satz 1, Abs. 2 Nr. 2
§ 9	§ 9 Satz 1	§ 9 Satz 1 Nr. 7 Anlage zu § 9	§ 9 Satz 1 Nr. 3, Nr. 4, Nr. 5 Anlage zu § 9	§ 9 Satz 1 Nr. 3, Nr. 4 Anlage zu § 9	§ 9 Satz 1 Nr. 8 Anlage zu § 9	§ 9 Satz 1 Nr. 1-6 Anlage zu § 9	§ 9 Satz 1
§ 10					§ 10 Abs. 2 Nr. 1	§ 10 Abs. 2, Abs. 3, Abs. 4 Satz 3	
§ 11	§ 11 Abs. 2 Satz 2 Nr. 10	§ 11 Abs. 2 Satz 2 Nr. 3	§ 11 Abs. 2 Satz 2 Nr. 3	§ 11 Abs. 2 Satz 2 Nr. 3 § 11 Abs. 2 Satz 2 Nr. 10	§ 11 Abs. 2 Satz 2 Nr. 2 § 11 Abs. 2 Satz 2 Nr. 10	§ 11 Abs. 2	§ 11 Abs. 2 Satz 2 Nr. 4

	Datenspar-samkeit	Verfügbar-keit	Integrität	Vertrau-lichkeit	Nichtver-kettbarkeit	Transpa-renz	Intervenier barkeit
§ 28, 28a	§ 28 Abs. 1 Satz 1 Nr. 1, Nr. 2, Abs. 2, Abs. 3 Satz 2, Abs. 6-9 § 28 a Abs. 1	§ 28 Abs. 3a Satz 1	§ 28 Abs. 3a Satz 1		§ 28 Abs. 1 Satz 1 Nr. 1, Nr. 2, Abs. 1 Satz 2, Abs. 2, § 28 Abs. 3 Satz 1, Satz 2, Satz 3, Satz 4, Satz 5, Satz 7, Abs. 5, Abs. 6-9 § 28a Abs. 1, Abs. 2, § 28a Abs. 2 Satz 4	§ 28 Abs. 3 Satz 4, Satz 5, § 28a Abs. 3 § 28a Abs. 2 Satz 2, Abs. 3	§ 28 Abs. 3a Satz 1, Abs. 4
§ 29					§ 29 Abs. 1, Abs. 2, Abs. 4	§ 29 Abs. 2 Satz 2, Satz 3, Satz 4, Abs. 7 Satz 1	§ 29 Abs. 3, Abs. 4
§ 30	§ 30 Abs. 1 § 30 a Abs. 3						
§ 31					§ 31		
§§ 33-35	§ 35					§§ 33, 34	§§ 33-35
§ 38						§ 38 Abs. 1 Satz 5	
§ 39					§ 39		
§ 40	§ 40				§ 40		
§ 42a						§ 42a	

6.2.2 Verankerung der Anwendbarkeit der Gewährleistungsziele auf personenbezogene Verfahren

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

Das BDSG enthält eine Reihe von Vorschriften, die das Verfahren als solches in den Blick nehmen und hierfür Anforderungen formulieren (vgl. §§ 4d Abs. 1, 4d Abs. 5, 6c Abs. 1, § 10 Abs. 1, § 28b Nr. 1, § 29 Abs. 2 S. 3, § 38 Abs. 5 S. 2, § 43 Abs. 2 Nr. 2 BDSG). Dabei werden

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

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

6.3 Verankerung der Gewährleistungsziele in den Landesdatenschutzgesetzen

Hier sind zunächst zwei Kategorien zu bilden. Etliche Landesdatenschutzgesetze sehen wie das BDSG bestimmte Kontrollen vor (HB, Hessen, RLP, Saarland, BY, BW und Niedersachsen). Für diese Länder ist auf die Ausführungen zum BDSG (oben 6.2) zu verweisen.

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

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

Dabei ist jedoch zu beachten, dass sich die gesetzlich vorgegebene Ausprägung des Schutzziels Transparenz von dem gleichlautenden Gewährleistungsziel unterscheidet. Während erstere lediglich die Dokumentation der Verfahrensweisen beinhaltet, umfasst letztere auch die Authentizität oder Revisionsfähigkeit konkreter Datenverarbeitungen sowie Informations-, Benachrichtigungs- und Auskunftsrechte (so bereits jetzt § 5 Abs. 1 Nr. 4 LDSG SH). Damit sind nur die Gewährleistungsziele „Nichtverkettbarkeit“, „Intervenierbarkeit“ und „Datensparsamkeit/-vermeidung“ nicht bereits in bestehenden Schutzzielen verankert. Hierzu kann jedoch auf die oben gemachten Ausführungen im Rahmen des BDSG verwiesen werden.

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

Datenspar-samkeit	**Verfügbar-keit**	**Integrität**	**Vertraulich-keit**	**Nichtverkett barkeit**	**Transparenz**	**Intervenierb arkeit**
§ 9 Abs. 1 Satz 2	§ 9 Abs. 2 Nr. 3	§ 9 Abs. 2 Nr. 2	§ 9 Abs. 2 Nr. 1		§ 9 Abs. 2 Nrn. 4-6	
§§ 20, 21 Abs. 2 Satz 2 (Löschung/ Sperrung bei entfallener Erforderlich-keit)				§ 4 Abs. 3 (Zweckfest-legung bei Einwilligung)	§ 4 Abs. 3 (informierte Einwilligung)	§ 4 Abs. 1 Nr. 2 (Einwilligung/ Rücknahme)
§ 36 Abs. 2 (Pseudo-nym./ Anonym. bei wiss. For-schung)				§ 10 Abs. 1 Nr. 2 (Zweckbe-stimmung im Verfahrens-verzeichnis)	§ 5 (Betrof-fenenrechte)	§§ 19-21 (Berichti-gung, Löschung, Sperrung)
§ 33 Abs. 4 (Löschfrist bei Videoauf-zeichnungen)				§ 12 Abs. 2, 5, 6 (Zweck-festleung bei Erhebung)	§3 10, 11 Abs. 4 Nr. 5, 31 Abs. 2 (Verfahrens-verzeichnis)	§ 32 Abs. 1 (Fernmessen und Fernwir-ken)
§ 12 (Erhebung nur bei Er-forderlichkeit)				§ 13 (Zweck-bindung bei Speicherung etc.)	§ 12 (Daten-erhebung)	
§ 13 (Spei-cherung etc. nur bei Er-forderlichkeit)				§§ 14 Abs. 3, 16 Abs. 4 (Zweckbin-dung bei Übermitt-lung)	§§ 18, 34 Abs. 3 (Auskunft)	
§§ 14, 15, 16, 17 (Übermitt-lung nur bei Erforderlich-keit)				§ 32 Abs. 1 (Zweckbin-dung bei Fernmessen und Fernwir-ken)	§ 27 (Kontrolle)	
				§ 33 (Zweck-bindung Video)	§ 32 (Fern-messen und Fernwirken)	
				§ 34 (auto-matisierte Einzelent-scheidung)	§ 33 Abs. 3 (Videoüber-wachung)	

6.4 Verankerung der Gewährleistungsziele in der EU-Datenschutzrichtlinie

Der Text zu diesem Abschnitt wird eingefügt, wenn die Kommentare aus der Artikel 29-Gruppe und der Technology Subgroup vorliegen.

7 Die generischen Maßnahmen zur Umsetzung der Gewährleistungsziele

Für jede der Komponenten des Standard-Datenschutzmodells (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 Gewährleistungsziele beitragen.

In diesem Abschnitt werden generische Datenschutz-Schutzmaßnahmen zu den jeweiligen Gewährleistungszielen aufgeführt, die in der Datenschutzprüfpraxis seit vielen Jahren erprobt sind und mit denen sich Datenschutzanforderungen bzw. die Gewährleistungsziele pragmatisch umsetzen lassen. Die konkreten Referenzmaßnahmen finden sich im Maßnahmenkatalog (im Anhang) wieder.

7.1 Gewährleistungsziel Datensparsamkeit

Das Gewährleistungsziel Datensparsamkeit kann erreicht werden durch:

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

7.2 Gewährleistungsziel 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 von Syntax und Semantik der Daten,
- Redundanz von Hard- und Software sowie Infrastruktur,
- Umsetzung von Reparaturstrategien und Ausweichprozessen,
- Vertretungsregelungen für abwesende Mitarbeiter.

7.3 Gewährleistungsziel Integrität

Typische Maßnahmen zur Gewährleistung der Integrität sind:

- Einschränkung von Schreib- und Änderungsrechten,
- Einsatz von Prüfsummen, elektronische Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptokonzepts,
- dokumentierte Zuweisung von Rechten 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.

7.4 Gewährleistungsziel Vertraulichkeit

Typische Maßnahmen zur Gewährleistung der Vertraulichkeit sind:

- Festlegung eines Rechte-Rollen-Konzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentisierungsverfahrens,
- Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal zugelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen,
- Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle,
- spezifizierte, für das Verfahren ausgestattete Umgebungen (Gebäude, Räume)
- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen etc.),
- Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept),
- Schutz vor äußeren Einflüssen (Spionage).

7.5 Gewährleistungsziel Nichtverkettbarkeit

Typische Maßnahmen zur Gewährleistung der Nichtverkettbarkeit sind:

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten,
- programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten,
- regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung,
- Trennung nach Organisations-/Abteilungsgrenzen,

- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentisierungsverfahrens,
- Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle,
- Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten,
- geregelte Zweckänderungsverfahren.

7.6 Gewährleistungsziel Transparenz

Typische Maßnahmen zur Gewährleistung der Transparenz sind:

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

7.7 Gewährleistungsziel Intervenierbarkeit

Typische Maßnahmen zur Gewährleistung der Intervenierbarkeit sind:

- differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten,
- Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen,
- dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verfahren sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes,
- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem,
- Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen,
- Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte,

- Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept,
- Einrichtung eines Single Point Of Contact (SPOC) für Betroffene,
- operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten,
- Einsichtsmöglichkeiten für die Datenschutzbeauftragten der verantwortlichen Stellen und die Datenschutz-Kontroll- und Aufsichtsbehörden.

8 Die Verfahrenskomponenten

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

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

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

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

Bei diesen drei Kernkomponenten spielen u.a. folgende Eigenschaften eine wesentliche Rolle:

Bei Daten sind Eigenschaften von **Datenformaten** zu betrachten, mit denen Daten erhoben und verarbeitet werden. Datenformate können Einfluss auf die Qualität der Umsetzung der Gewährleistungsziele haben, bspw. in den Fällen, in denen nicht als abschließend geklärt gelten darf, welche Inhalte Dateien mit bestimmten Formaten aufweisen oder wenn es sich um verlustbehaftete Dateien handelt.

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

Für jeden Prozess gilt es Verantwortlichkeiten zu klären, die typischerweise als Rolle in einem umfassenden Rollenkonzept formuliert und zugewiesen sind. Die Verantwortlichkeit eines Prozesseigentümers erstreckt sich auf Kernprozesse und Hilfsprozesse im Bereich von

Technik und organisatorischen Regelungen oder im Bereich der inhaltlich geprägten Datenverarbeitung oder durchgängig über alle Prozessebenen eines Verfahrens hinweg im Sinne einer Gesamtverfahrensverantwortlichkeit. Diese Verantwortlichkeit kann auf unterschiedliche Rollen verteilt werden. Der Bezug von Prozess- und Verfahrensverantwortlichkeit ist von entscheidender Bedeutung für die Zuordnung, welche beteiligte Instanz für die Ordnungsmäßigkeit eines Verfahrens zur Datenverarbeitung aktiv zu sorgen hat.

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

9 Der Schutzbedarf

9.1 Die Schutzbedarfsabstufungen

Jede Verarbeitung personenbezogener Daten bedarf einer gesetzlichen Regelung oder einer wirksamen Einwilligung des Betroffenen. Die Ermittlung des Schutzbedarfs eines Verfahrens ist deshalb nur unter der Voraussetzung sinnvoll, dass eine Ermächtigungsgrundlage vorliegt, die das Verbot mit Erlaubnisvorbehalt für den ausgewiesenen Zweck aufhebt. Bei der Ermittlung des Schutzbedarfs ist im Unterschied zu Informationssicherheitsstandards, welche die Daten verarbeitende Organisation im Fokus haben, die Perspektive des Betroffenen einzunehmen. Aus der Machtasymmetrie zwischen potenziell übermächtiger Organisation und dem Individuum ergeben sich auch die anders definierten und erweiterten datenschutzrechtlichen Gewährleistungsziele, welche der Wahrnehmung und Verteidigung der Grundrechte der schwächeren Position dienen.

9.2 Objektbereiche

Der Schutzbedarf ist – bezogen auf die einzelnen Gewährleistungsziele – für unter Punkt 8 bereits beschriebenen Komponenten Daten, Systeme und Prozesse zu betrachten. Der Schutzbedarf der Daten vererbt sich dabei auf Systeme und Prozesse, wobei stets auf Kulminierungseffekte geachtet werden muss, wenn z. B. Daten in großem Umfang an einer räumlichen Stelle verarbeitet werden oder einzelne Prozesse besonders Risiko behaftet sein können.

9.3 Definition der Schutzbedarfskategorien

Es werden drei Schutzbedarfskategorien unterschieden:

- Normal: Schadensauswirkungen sind begrenzt und überschaubar und etwaig eingetretene Schäden für Betroffene relativ leicht durch eigene Aktivitäten zu heilen,
- Hoch: die Schadensauswirkungen werden für Betroffene als beträchtlich eingeschätzt, z.B. weil der Wegfall einer von einer Organisation zugesagten Leistung die Gestaltung des Alltags nachhaltig veränderte und der Betroffene nicht aus eigener Kraft handeln kann sondern auf Hilfe angewiesen wäre,
- Sehr hoch: Die Schadensauswirkungen nehmen ein unmittelbar existentiell bedrohliches, katastrophales Ausmaß für Betroffene an.

9.4 Schadensszenarien für Betroffene

Die Schadensszenarien orientieren sich am BSI-Standard 100-2 (https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30748/standard_1002_pdf.pdf; ab Seite 49), werden aber grundsätzlich aus Sicht des Betroffenen bzw. potenziell Geschädigten betrachtet. Das Schadensszenario „Beeinträchtigung der Aufgabenerfüllung“ wird dabei nicht betrachtet, da dies ein eher auf Seiten einer Organisation, nicht

eines Individuums, zu verortender Schaden ist. Stattdessen wird ein Schadensszenario „Auswirkungen auf nicht unmittelbar Betroffene (Grundrechtsausübung)“ eingeführt. Dies soll Schäden transparent machen, die gesellschaftliche Auswirkungen haben, die sich auf die Grundrechtsausübung auch nicht unmittelbar Betroffener auswirken.

1. Unrechtmäßige Datenverarbeitung (Verstoß gegen Gesetze/Vorschriften/Verträge)
2. Beeinträchtigungen für informationelle Selbstbestimmung
3. Beeinträchtigungen des Ansehens und der Reputation des/der Betroffenen
4. Finanzielle Auswirkungen für den/die Betroffenen
5. Beeinträchtigungen der persönlichen Unversehrtheit des/der Betroffenen
6. Auswirkungen auf nicht unmittelbar Betroffene (Grundrechtsausübung)

Schutzbedarfskategorie „normal“	
1. Unrechtmäßige Datenverarbeitung (Verstoß gegen Gesetze/Vorschriften/ Verträge)	Transparente unrechtmäßige Datenverarbeitung im anzunehmenden Interesse des Betroffenen, Interventionsmöglichkeit des Betroffenen vorhanden.
2. Beeinträchtigungen für informationelle Selbstbestimmung	Verarbeitung personenbezogener Daten des Betroffenen.
3. Beeinträchtigungen des Ansehens und der Reputation des/der Betroffenen	Eine geringe bzw. nur interne Ansehens- oder Reputationsbeeinträchtigung ist möglich, Interventionsmöglichkeiten für den Betroffenen sind vorhanden.
4. Beeinträchtigungen der persönlichen Unversehrtheit des/der Betroffenen	Eine Beeinträchtigung erscheint nicht möglich.
5. Finanzielle Auswirkungen für den/die Betroffenen	Der finanzielle Schaden bleibt für den Betroffenen tolerabel oder kann vom Verursacher oder Dritten restituiert werden.
6. Auswirkungen auf nicht unmittelbar Betroffene (Grundrechtsausübung)	Erhebliche negative gesellschaftliche Auswirkungen sind nicht ausgeschlossen.

Schutzbedarfskategorie „hoch“	
1. Unrechtmäßige Datenverarbeitung (Verstoß gegen Gesetze/Vorschriften/Verträge)	Unrechtmäßige Datenverarbeitung, die erwartbar nicht im Interesse des Betroffenen liegt
2. Beeinträchtigungen für informationelle Selbstbestimmung	Verarbeitung personenbezogener Daten des Betroffenen, die einen weitreichenden Einblick in dessen Persönlichkeit oder dessen mögliches Verhalten und Handeln erlauben.
3. Beeinträchtigungen des Ansehens und der Reputation des/der Betroffe-	Eine Ansehens- oder Reputationsbeeinträchtigung ist zu er-

nen	warten, Interventionsmöglichkeiten für den Betroffenen sind beschränkt, bei der er auf externe Hilfe angewiesen ist.
4. Beeinträchtigungen der persönlichen Unversehrtheit des/der Betroffenen	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.
5. Finanzielle Auswirkungen für den/die Betroffenen	Der Schaden bewirkt beachtliche finanzielle Verluste für den Betroffenen, ist jedoch noch nicht existenzbedrohend.
6. Auswirkungen auf nicht unmittelbar Betroffene (Grundrechtsausübung)	Erhebliche negative gesellschaftliche Auswirkungen sind zu befürchten.

Schutzbedarfskategorie „sehr hoch“	
1. Unrechtmäßige Datenverarbeitung (Verstoß gegen Gesetze/Vorschriften/Verträge)	Unrechtmäßige Datenverarbeitung, die dem Interesse des Betroffenen klar widerspricht und unmittelbare konkrete negative Folgen hat.
2. Beeinträchtigungen für informationelle Selbstbestimmung	Verarbeitung besonders schützenswerter personenbezogener Daten des Betroffenen, die dazu führen, dass ein Betroffener weitestgehend von den Aktivitäten einer Organisation gesteuert und davon abhängig wird.
3. Beeinträchtigungen des Ansehens und der Reputation des/der Betroffenen	Ein starke Ansehens- oder Reputationsbeeinträchtigung ohne Interventionsmöglichkeiten für den Betroffenen, eventuell sogar Existenz gefährdender Art, ist denkbar.
4. Beeinträchtigungen der persönlichen Unversehrtheit des/der Betroffenen	Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich, mit Gefahr für Leib und Leben.
5. Finanzielle Auswirkungen für den/die Betroffenen	Der finanzielle Schaden ist für den Betroffenen existenzbedrohend.
6. Auswirkungen auf nicht unmittelbar Betroffene (Grundrechtsausübung)	Erhebliche negative gesellschaftliche Auswirkungen sind zu erwarten.

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.

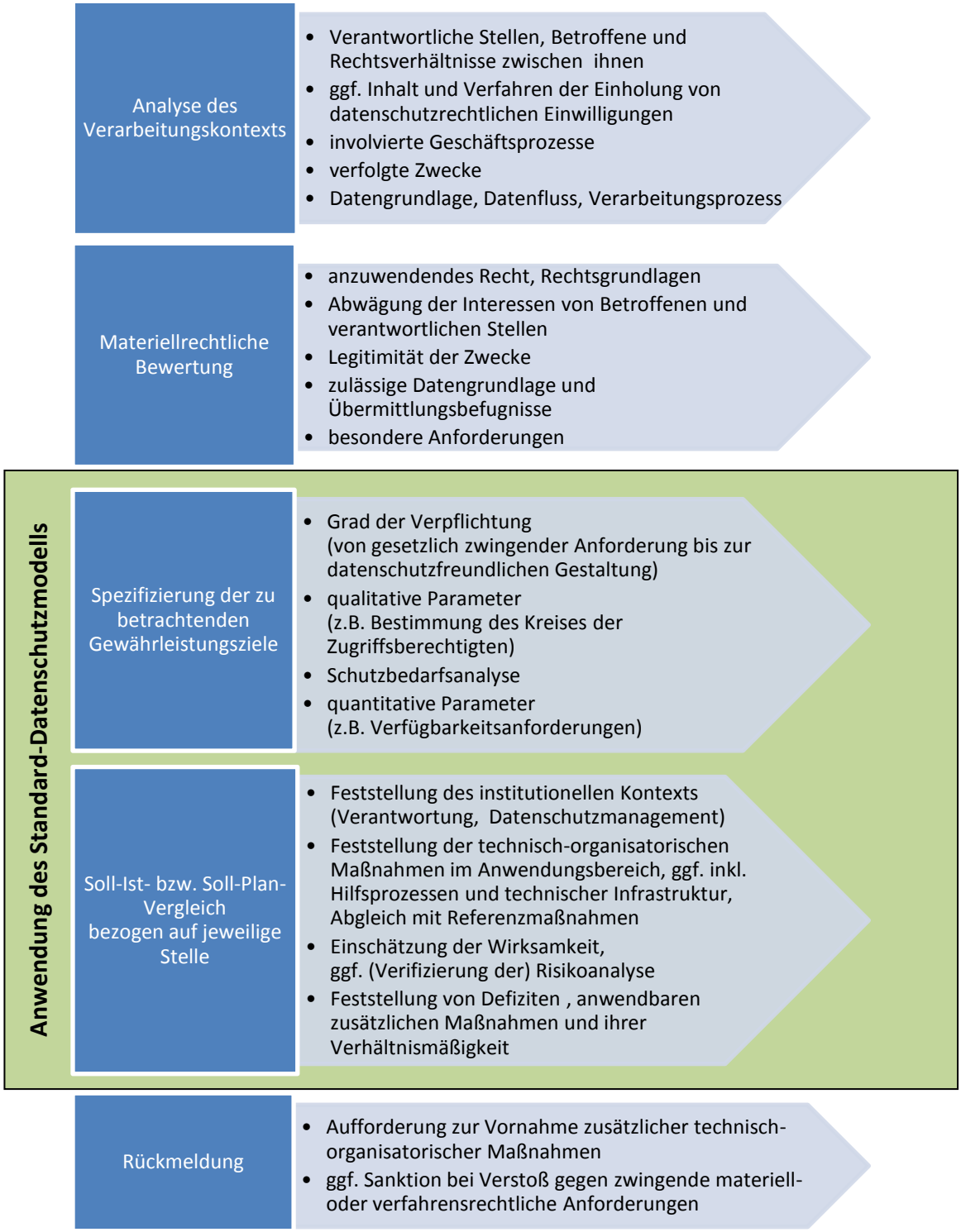

Abbildung 1: Die Anwendung des Standard-Datenschutzmodells im Rahmen von Prüf- und Beratungsvorgängen

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

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

Für die Anwendung des Standard-Datenschutzmodells 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 Standard-Datenschutzmodells zur Beurteilung der vorgenommenen oder geplanten technischen und

organisatorischen Maßnahmen basieren auf der Feststellung der sachlichen Verhältnisse der Verarbeitung. Hierzu gehören insbesondere die Fragen:

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

Ausführlichkeit und Detaillierungsgrad der Feststellung der sachlichen Verhältnisse werden von Vorgang zu Vorgang variieren, ebenso wie der Grad der Formalisierung des Vorgehens von informeller Befragung bis hin zum Einsatz von standardisierten Fragebögen. Eine strukturierte Zusammenfassung der Ergebnisse ist dennoch ebenso üblich wie für die weiteren Schritte unentbehrlich.

Die sich an die Feststellung der sachlichen Verhältnisse anschließende materiellrechtliche Bewertung beurteilt, inwieweit die geprüfte oder vorgesehene Verarbeitung grundsätzlich zulässig ist. Darüber hinaus gibt sie Antworten auf folgende Fragen, die für die folgende Anwendung des Standard-Datenschutzmodells 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 Spezifizierung der Gewährleistungsziele

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

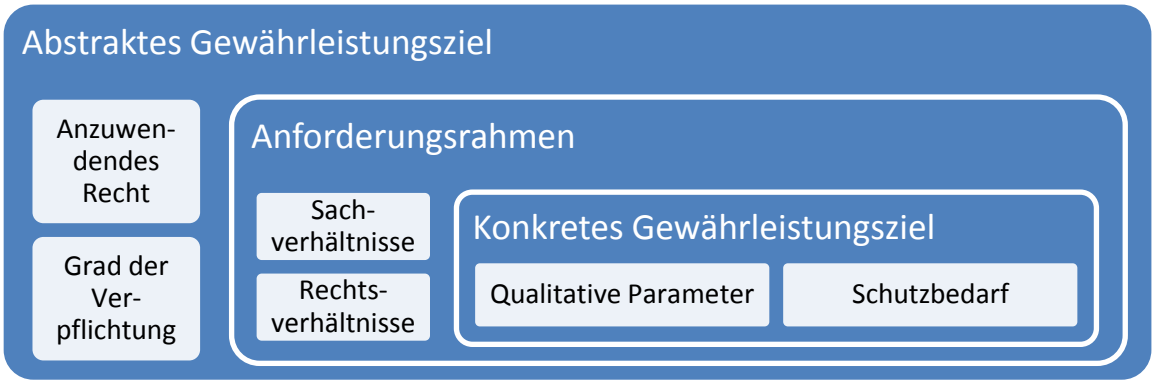

Abbildung 2: Spezifizierung der Gewährleistungsziele

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

1. *Innerhalb von welchen Prozessen ist für wen die Verfügbarkeit von welchen Daten zu gewährleisten?* Der Einfluss der Möglichkeit der ordnungsgemäßen Verwendung der Daten auf die Interessen der Betroffenen ist der Maßstab für die Konkretisierung des Gewährleistungsziels der Verfügbarkeit. Das Gewährleistungsziel erstreckt sich nur auf solche Daten und diejenigen Geschäftsprozesse, bei denen ein Verlust der Verfügbarkeit den Interessen der Betroffenen zuwiderläuft.
2. *Welche Daten sollen unversehrt, welche aktuell gehalten werden?* Auch hier ist das Interesse der Betroffenen der Maßstab. In Bezug auf die Gewährleistung der Aktualität ist in die Abwägung einzubeziehen, dass Aktualität in der Regel nur mit zusätzlichen Erhebungs- und Verarbeitungsvorgängen zu erhalten sein wird, deren Durchführung u. U. anderen Interessen der Betroffenen zuwiderlaufen können.
   Inwieweit die Integrität der Prozesse und Systeme zu gewährleisten ist, leitet sich aus der Konkretisierung der anderen Gewährleistungsziele ab.
3. *Wem ist die Kenntnisnahme welcher Daten zu verwehren?* Das Ausmaß des befugten Zugriffs ist zunächst technikunabhängig aus den jeweiligen Geschäftsprozessen abzuleiten. Hiermit ist der Rahmen bestimmt, innerhalb dessen sich die Maßnahmen zum Vertraulichkeitsschutz gegenüber unbefugten Beschäftigten der verantwortlichen Stellen zu

bewegen haben. Der Rahmen für die Kenntnisnahme Dritter ist durch die in der materiell-rechtlichen Analyse festgestellten Übermittlungsbefugnisse gegeben.

4. *Für wen ist die Datenverarbeitung in welcher Form transparent zu halten?* Es sind Anforderungen an die Verfahrensdokumentation nach § 4e BDSG, an die interne Dokumentation der Verarbeitungsvorgänge und deren Auswertbarkeit sowie an die Revisionsfähigkeit der Verarbeitung festzuhalten.
5. *Welche Betroffenenrechte sind in welcher Ausprägung zu gewähren?* Welche Betroffene müssen von der automatisierten Verarbeitung benachrichtigt werden? Welche Daten sind in die Beauskunftung unter welchen Bedingungen einzubeziehen? Unter welchen Bedingungen sind die Daten zu löschen bzw. zu sperren?
6. *Welche Zweckänderungen sind zulässig? Welche Zwecke von Hilfsprozessen leiten sich aus den Kernprozessen legitim ab?* Benötigt werden lediglich Aussagen zu solchen Zwecken, welche die verantwortlichen Stellen tatsächlich verfolgen bzw. zu verfolgen beabsichtigen. Maßnahmen zur Gewährleistung der Nichtverkettbarkeit sollen mit dem Ziel ergriffen werden, die Verarbeitung oder Nutzung der Daten für alle außer den festgelegten legitimen Zwecken auszuschließen.
7. *Die Kenntnisnahme von und die Ausübung welcher Verfügungsgewalt über welche Daten der Betroffenen durch welche Personen und Stellen sind zu minimieren?* Ausgangspunkt sind erneut die Interessen der Betroffenen, auch innerhalb einer Verarbeitung zu legitimen Zwecken die Belastung auf das erforderliche Maß zu begrenzen.

Nachdem die Gewährleistungsziele qualitativ feststehen, muss eine Schutzbedarfsanalyse erfolgen bzw. die Schutzbedarfsanalyse der verantwortlichen Stelle(n) nachvollzogen werden. Die Vorgehensweise ist in Kapitel 9 niedergelegt. Ihr Ergebnis fließt in dreierlei Form in die weiteren Betrachtungen ein.

Zum Ersten können die Gewährleistungsziele quantitativ näher bestimmt werden. Beispiele für Präzisierungen sind Antworten auf folgende Fragen: Für welchen Zeitraum ist der Verlust der Verfügbarkeit der Daten für die Betroffenen in welchem Grad tolerabel? Mit welcher Verzögerung soll die Aktualität der Daten garantiert werden? Mit welcher zeitlichen Präzision muss die Verarbeitung im Nachhinein nachvollzogen werden können? In welchem zeitlichen Rahmen muss die verantwortliche Stelle in der Lage sein, die jeweiligen Betroffenenrechte zu gewähren?

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

Zum Dritten fließt das Ergebnis der Schutzbedarfsanalyse in die Bewertung der Restrisiken ein, die nach Umsetzung der Maßnahmen verbleiben, die mit einem Aufwand ergriffen werden können, der in angemessenem Verhältnis zum Zweck der Verarbeitung besteht. Diese Risiken hängen regelmäßig von dem Interesse von Dritten oder von Verfahrensbeteiligten

ab, die Gewährleistungsziele zu verletzen, sei es um Daten der Betroffenen unbefugt zur Kenntnis zu nehmen, um sie für illegitime Zwecke, über das erforderliche Maß hinaus oder in intransparenter Weise zu erheben, zu nutzen, zu speichern, zu übermitteln oder anderweitig zu verarbeiten.

10.3 Der Soll-Ist-Vergleich

Der Kern der Anwendung des Standard-Datenschutzmodells besteht in dem Vergleich der Referenzmaßnahmen, die sich aus den betrachteten und wie oben konkretisierten Gewährleistungszielen ableiteten lassen, mit den von der verantwortlichen Stelle geplanten bzw. in der Prüfung festgestellten Maßnahmen. Abweichungen sind danach zu gewichten und zu beurteilen, inwieweit sie das Erreichen der Gewährleistungsziele gefährden. In einem Prüfvorgang erlaubt die bis zu diesem Punkt geführte Analyse aus einem Verfehlen der Gewährleistungsziele auf (ggf. sanktionierbare) datenschutzrechtliche Mängel zu schließen.

In der Prüf- und Beurteilungspraxis lässt sich häufig mit nur geringem Aufwand feststellen, dass Anforderungen nicht erfüllt werden, weil die entsprechend zugeordneten Maßnahmen sofort ersichtlich fehlen. Komplizierter ist der Fall, wenn die zu prüfende Stelle andere als die Referenzschutzmaßnahmen gewählt hat. Auch wenn diese als grundsätzlich geeignet beurteilt werden können, kann in Zweifel stehen, dass sie in ihrer konkreten Ausgestaltung 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 des Grundbetriebs,
- Schaffung von Transparenz hinsichtlich der Veröffentlichung und Weiterentwicklung des Modells

11.2 Auftraggeber, Projektleitung, Anwender

Der Auftraggeber für die Entwicklung und Pflege des SDM ist die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** (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 Beauftragten für den Datenschutz der Länder und des Bundes (AK Technik). Der AK Technik hat die Projektleitung inne.

Die Anwender des SDM sind im Wesentlichen die sechzehn Landesdatenschutzbeauftragten, das bayerische Landesamt für Datenschutzaufsicht sowie die Bundesdatenschutzbeauftragte im Rahmen ihrer gesetzlichen Beratungs-, Prüf und Sanktionstätigkeiten (**Anwendergruppe 1**). Weitere Anwender des SDM sind die behördlichen und betrieblichen Datenschutzbeauftragten (**Anwendergruppe 2**).

Das Modell wird wie folgt weiterentwickelt:

- Erstellung und Pflege des SDM-Handbuchs , das auch den Katalog von Referenz-Schutzmaßnahmen umfasst;
- Bereitstellung des SDM-Handbuchs 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-Handbuchs;
- 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 Schutzmaßnahmen-Referenzkatalog

Der Schutzmaßnahmen-Referenzkatalog ist als **Anhang A** Bestandteil des Handbuches, wird aber, in Abhängigkeit der technischen Entwicklung, in kürzeren Zyklen nach den Vorgaben des Betriebsmodells (siehe Kapitel 11) überarbeitet als das Handbuch selbst.