AK Technik-Workshop 2015

**„Das Standard-Datenschutzmodell –
der Weg vom Recht zur Technik"**

Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen

Tagungsband

Mittwoch, 29. April 2015,
Bundesanstalt für
Geowissenschaften und
Rohstoffe (BGR), Hannover

IMPRESSUM

Tagungsband
„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen
(Mittwoch, 29. April 2015,
Bundesanstalt für Geowissenschaften und Rohstoffe (BGR), Hannover)

Herausgeber:
AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

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

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

Inhalt

Vorwort

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (AK Technik) veranstaltet jährlich einen fachübergreifenden Workshop zu einem aktuellen Datenschutzthema. Eingeladen sind neben den Mitgliedern des AK Technik insbesondere die Juristinnen und Juristen aller Dienststellen. Wesentliches Ziel dieser Workshops ist es, Juristen mit technischen Themen vertraut zu machen und Techniker an juristische Sachverhalte heranzuführen.

Diese Workshops haben Tradition. Der erste Workshop dieser Reihe fand im Jahr 2006 in Frankfurt zum Thema digitale Signatur statt. Als Referenten waren u. a. Professor Beutelspacher und Professor Roßnagel eingeladen, um die mathematischen und juristischen Grundlagen digitaler Signaturen zu erläutern. Im Workshop des Jahres und 2007 beleuchtete der Workshop verschiedene Aspekte des Datenschutzmanagements und 2008 stand der elektronische Reisepass im Mittelpunkt. Besonders hervorzuheben ist der Workshop im Jahr 2009. Die Professoren Pfitzmann, Bäcker und Kutscha waren meiner Einladung nach Berlin gefolgt, um den Teilnehmern des Workshops auf nachhaltige Weise verschiedene Aspekte des neuen IT-Grundrechts zu erläutern. In den folgenden Jahren standen Themen wie der neue Personalausweis, IPv6 oder BYOD auf der Agenda der Workshops.

In diesem Jahr hatte der AK Technik eingeladen, um den Stand der Entwicklung des Standard-Datenschutzmodells (SDM) zu erläutern und zur Diskussion zu stellen. Die Datenschutzkonferenz hat den AK Technik beauftragt, das SDM zu entwickeln. Ziel des SDM ist es, die rechtlichen Anforderungen der Datenschutzgesetzgebung von Bund und Ländern in die Gewährleistungsziele Datensparsamkeit, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit zu überführen und daraus einen Katalog mit standardisierten Datenschutzmaßnahmen abzuleiten. Auf diese Weise lassen sich aus den rechtlichen Anforderungen insbesondere Maßnahmen zur Gewährleistung eines angemessenen Datenschutzes ableiten. Da sich das SDM methodisch an den IT-Grundschutz anlehnt, können auch Maßnahmen zur Gewährleistung der erforderlichen Informationssicherheit ausgewählt und auf ihre Datenschutzkonformität und Ordnungsmäßigkeit hin bewertet werden. Im Ergebnis soll das SDM auch bewirken, dass die datenschutzrechtlichen Anforderungen möglichst bundesweit einheitlich und für die verantwortlichen Stellen leicht nachvollziehbar sind.

Das SDM soll auch dazu beitragen, dass die deutschen Datenschutzaufsichtsbehörden auf europäischer Ebene mit einer Stimme sprechen. Das SDM soll mit Blick auf die Entwürfe der europäischen Datenschutz-Grundverordnung einen Weg aufzeigen, wie auch künftig ein an Grundrechten orientierter Datenschutz durchgesetzt werden kann. Auch vor diesem Hintergrund wird das SDM ins Englische übersetzt. Eine Kurzversion der Übersetzung ist diesem Tagungsband beigefügt.

Die 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Oktober 2014 die Version 0.8 des SDM-Handbuchs verabschiedet. Auf dieser Version des Handbuchs basierten alle Vorträge, die während des Workshops gehalten wurden und die in diesem Tagungsband zusammengefasst sind. Mit der bewussten Publizierung eines Zwischenstandes des SDM im Tagungsband soll verdeutlicht werden, dass die Arbeit am Handbuch keinesfalls abgeschlossen ist. Vielmehr möchte der AK Technik alle Leserinnen und Leser dazu aufrufen, den Text zu kommentieren und Änderungs- und Ergänzungsvorschläge zu unterbreiten.

Die Liste der Referentinnen und Referenten dieses Workshops macht deutlich, dass das SDM nicht ausschließlich ein technisches Thema ist. In der vom AK Technik eingesetzten Arbeitsgruppe entwickeln Juristinnen und Juristen gemeinsam mit Technikerinnen und Technikern das Standard-Datenschutzmodell. Dies führt mitunter zu spannenden und kontroversen aber immer konstruktiven Diskussionen, die stets geprägt sind vom Willen, gemeinsame Lösungen zu finden.

Ich möchte die Gelegenheit nutzen, mich schon heute ganz herzlich bei allen Mitgliedern der Arbeitsgruppe für die konstruktive Zusammenarbeit zu bedanken. Mein besonderer Dank gilt Martin Rost vom ULD Schleswig-Holstein als Leiter der Arbeitsgruppe, der uns mit seinem Enthusiasmus und seiner Begeisterung für das SDM angesteckt und immer wieder motiviert hat, die Arbeit am Modell voranzutreiben. Bedanken möchte ich mich auch bei Uwe Robra und seinem Team vom LfD Niedersachsen, der die Organisation des Workshops vor Ort in Hannover übernommen hat.

Abschließend möchte ich nochmals alle Leserinnen und Leser dieses Tagungsbandes dazu aufrufen, das Handbuch und die Vortragsfolien kritisch zu lesen und zu kommentieren. Das SDM-Team freut sich auf Ihre Änderungs- und Ergänzungswünsche und steht für Fragen und Hinweise zum Standard-Datenschutzmodell gerne zur Verfügung.

Gabriel Schulz
(Leiter des AK Technik)

AK Technik-Workshop 2015

„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen

Mittwoch, 29. April 2015, 11:00 – 16:00 Uhr

Bundesanstalt für Geowissenschaften und Rohstoffe (BGR), Geozentrum Hannover, Stilleweg 2, Großer Sitzungssaal, 30655 Hannover

---

11:00	**Eröffnung** Gabriel Schulz Mecklenburg-Vorpommern
11:10	**Geschichte und Grundzüge des Standard-Datenschutzmodells** Martin Rost Schleswig-Holstein
11:30	**Das BDSG als Basis für das Standard-Datenschutzmodell/ Verankerung der Gewährleistungsziele in den Landesdatenschutzgesetzen** Meike Kamp / Dr. Tino Naumann Berlin / Sachsen
12:00	**Der europäische Bezug des Standard-Datenschutzmodells** Kirsten Bock Schleswig-Holstein
12:30	**Fragen und Diskussion**
13:00	*Mittagspause*
14:00	**Das Zusammenspiel von Recht und Technik** Dr. Ulrich Vollmer Berlin
14:20	**Vorstellung eines Fallbeispiels aus dem öffentlichen Bereich** Uwe Robra/Michael Wilms Niedersachsen / Nordrhein-Westfalen
14:40	**Vorstellung eines Fallbeispiels aus dem privaten Bereich** Lars Konzelmann Sachsen
15:00	**Diskussion**
15:45	**weiterer Zeitplan** Martin Rost Schleswig-Holstein
15:55	**Schlusswort** Reinhard Dankert Mecklenburg-Vorpommern

Geschichte und Grundzüge des Standard-Datenschutzmodells*

Martin Rost, ULD

29.04.2015, Hannover

Mit * in der Folienüberschrift ausgezeichnete Folien wurde nachträglich eingefügt. Diese Folien waren aus Zeitgründen aus dem Vortrag ausgeblendet worden.

Zur methodischen Vorgeschichte des SDM…

- 1992, März: Das BSI veröffentlicht die erste Version des „IT-Sicherheitshandbuchs (BSI 7105)“
- 1994: IT-Sicherheitshandbuch V2 sucht methodische Orientierung an den drei Schutzzielen **Verfügbarkeit, Integrität und Vertraulichkeit**
- 1995: EU verabschiedet **Datenschutzrichtlinie**

BDSG-Gutachten und LDSG-Novellen mit Schutzzielen, Privacy-By-Design (2001/2002)

- Garstka/ Pfitzmann/ Rossnagel empfehlen im „**Gutachten** zur Modernisierung des deutschen Datenschutzrechts“ die Nutzung von „Schutzzielen“.
- Die neuen Bundesländer sowie Hamburg, Berlin und NRW weisen in ihren **reformierten Landesdatenschutzgesetzen** Schutzziele aus.
- Prof. Pfitzmann/ Dr. Fedderath (Lehrstuhl Informationssicherheit und Datenschutz der TU-Dresden) veröffentlichen einen Artikel zur **Systematik der Schutzziele**

  Bezug: „Orange Book“ (DoD 1985), Deutsche IT-Sicherheitsbewertungskriterien (1989), ITSEC (1991), Kanadische Kriterien (1992), Common Criteria, ISO/IEC 15408
- Erste Umsetzungen von Ideen zu „Privacy-Enhancing-Technologies“ und „Privacy-By-Design“ zeichnen sich im kontinental-europäischen **Datenschutzdiskurs** ab.

IT-Grundschutz Prozesse (2007)

- Datenschutz-Anforderungen werden im IT-Grundschutzkatalog des BSI im **Baustein 1.5** aufgenommen:
  - 13 spezifische Datenschutzgefährdungen
  - 16 Datenschutz-Maßnahmen
  - Initiative aus dem AK-Technik heraus (Federführung Saarland, Herr Simon)
  - Ergebnis: **Datenschutz wird faktisch zur Untermenge von IT-Sicherheit**
- Operativer Datenschutz setzt sich mit **Prozessstandards** wie ITIL, CoBIT, SAGA sowie ISO auseinander
  - DuD-Aufsätze wie „Datenschutz durch Prozessmodellerung“ (Dr. Meints)
  - Gut besuchte Veranstaltung des AK-Technik zu Prozess(modellierungen) in Hannover
  - IT-Sicherheitsmanagement wird standardisiert (bis zur ISO 27001)
  - Ergebnis: **Prozesse werden zur eigenständigen Prüf- und Gestaltungskategorie des Datenschutzes**

SDM
Standard-Datenschutzmodell

BVerfG formuliert Schutzziele-Urteil (2008)

- Februar: Das BVerfG fällt das **Integritäts- und Vertraulichkeitsurteil**

  Der Staat hat die Umsetzung der Schutzziele Vertraulichkeit und Integrität zu gewährleisten (nach gründlicher Diskussion zwischen Prof. Pfitzmann und Prof. Papier (Präsident des BVerfG)).
- November: Prof. Pfitzmann schickt Frau Hansen (ULD) ein internes **Arbeitspapier** mit einer Kritik an bisherigen Schutzzielkonzepten. Das ULD springt, im Unterschied zu den Assistenten von Prof. Pfitzmann, sofort an und sieht das Potential der Systematisierung der Schutzmaß-nahmen des Datenschutzes.

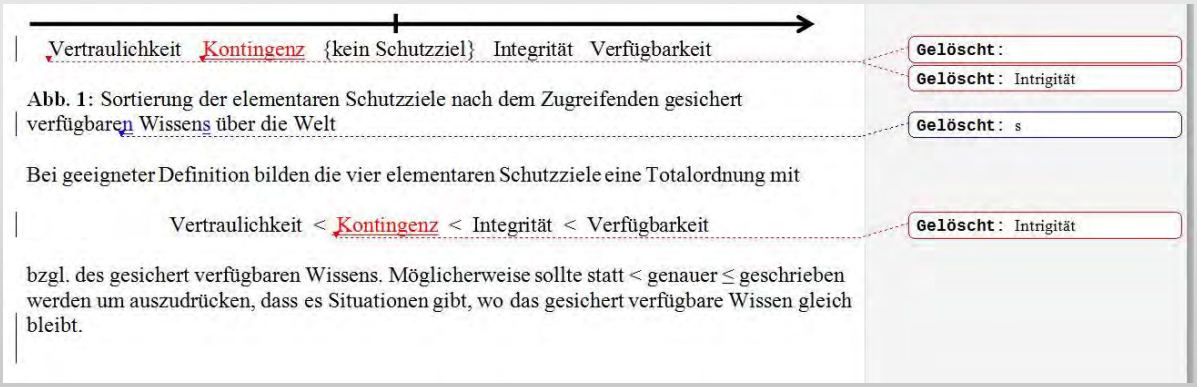
SDM
Standard-Datenschutzmodell

Kritik an den bislang vorgelegten Schutzziel-Konzepten (2009)

Die bisherigen Publikationen zu Schutzzielen

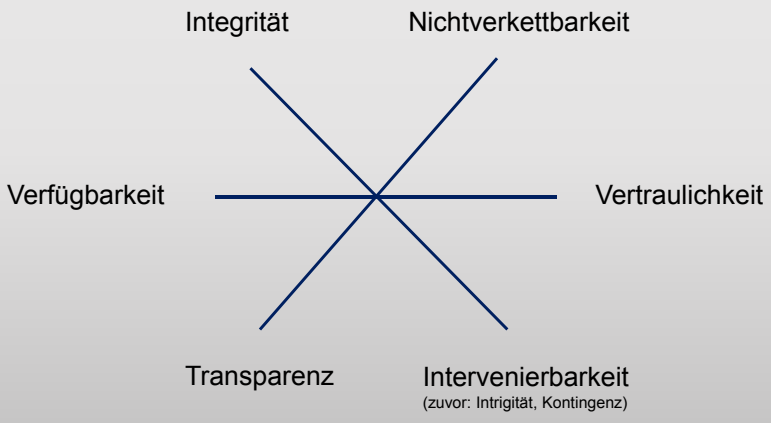
1. bringen **keine Struktur** in den Raum der Schutzziele;
2. untersuchen **keine Wechselwirkungen**, d.h. ob und inwiefern sich Schutzziele gegenseitig verstärken oder schwächen oder gar implizieren oder gegenseitig ausschließen;
3. enthalten **keine Überlegungen zur Vollständigkeit** der Schutzziele oder zu einem **erzeugenden System**.

Erster Entwurf einer eindimensionalen Anordnung der Schutzziele (2009)



Aus: **„Schutzziele noch mal ganz von vorn“** Andreas Pfitzmann TU Dresden, Fakultät Informatik, Version 0.21 vom 11.04.2009 (internes Arbeitspapier)

Zweiter Entwurf einer Anordnung der Schutzziele (2009)

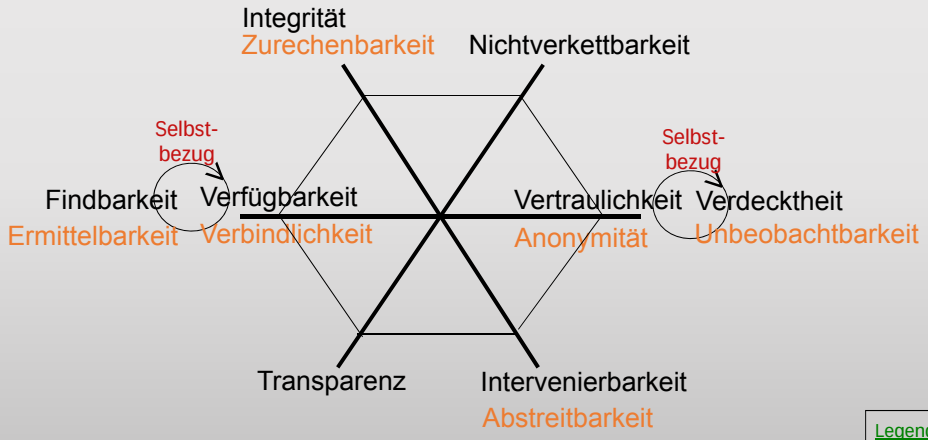


Bezug zum Schutzzielekatalog der 1. Generation:

Authentizität wird dem Schutzziel Integrität und **Revisionsfähigkeit** den Schutzzielen zur Sicherung der Integrität und Transparenz subsummiert.

SDM
Standard-Datenschutzmodell

Vollständige Systematik der Schutzziele*



Legende:
Informations-Inhalte
Informationsumfeld

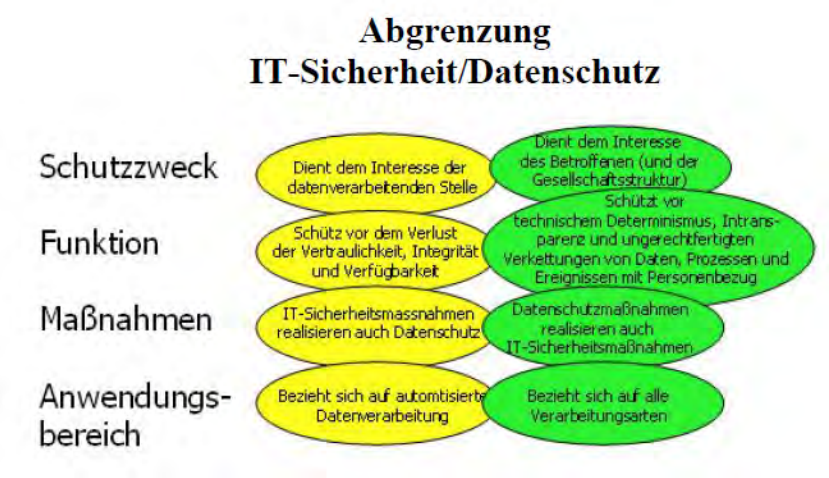
SDM
Standard-Datenschutzmodell

Erste Festlegungen zu Schutzzielen (2009)

- Diskussion führt zur Ablösung des eindimensionalen Entwurfs durch einen „3-Achsen-Entwurf".
- Rost/ Pfitzmann publizieren einen Artikel in der DuD
  (2009/06: 353ff: „Datenschutz-Schutzziele revisited")
- Ergebnisse des „**Magdeburger-Treffens**":
  - Die Schutzzielbezeichnung „Kontingenz" ist schlecht vermittelbar, deshalb: „Intervenierbarkeit".
  - Erarbeitung *datenschutzspezifischer* Definitionen der sechs Schutzziele.
  - Schutzziele werden aus rechtliche Anforderungen abgeleitet, nicht wie bislang an Regelwerke der Informationssicherheit gekoppelt.
  - Der Fokus wird von „personenbezogenen Daten" auf „personenbezogene Verfahren" ausgeweitet.


Datenschutz-Schutzziele – revisited

1. konsolidiertes Papier des AK-Technik zu Schutzzielen (2009



Unterscheidung von IT-Grundschutz und operativem Datenschutz

Quelle: Arbeitskreis „Technische und organisatorische Datenschutzfragen“: Empfehlungen für die Vereinheitlichung der Regelungen zum technischen und organisatorischen Datenschutz - Zwischenbericht – (20.08.2009), Grafikentwurf: Walter Ernestus, BfDI

Situation 2010*

- Vorstellung des Schutzzielekonzepts auf dem „AK Verwaltungsmodernisierung“ beim BfDI in Bonn
- Veröffentlichung des **Positionspapiers** der 79. DSK „Ein modernes Datenschutzrecht für das 21. Jahrhundert“: Konkrete Schutzziele und Grundsätze verankern**:**

  „Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sollten als allgemeingültige datenschutzrechtliche Grundregelungen einen verbindlichen Mindeststandard festlegen. Sie sollten allgemeine Vorgaben enthalten, die als Grundlage aller datenschutzrechtlichen Regelungen und Maßnahmen für öffentliche und nichtöffentliche Stellen dienen. Ausgehend von den Schutzzielen sollten sanktionsbewehrte Grundsatznormen formuliert werden, die für alle Formen der Datenverarbeitung gleichermaßen gelten.“
- Die Einflussnahme auf den Standard **ISO29100 / 29101** scheitert (weil international nur der kleinste Kompromiss einer bloßen Sammlung von 11 privacy principles - einer Mischung aus „Prinzipien“, normativen Anforderungen und Maßnahmen - erzielbar war).

SDM
Standard-Datenschutzmodell

Konferenz der Datenschutzbeauftragten (2010)


Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Ein modernes Datenschutzrecht für das 21. Jahrhundert

Eckpunkte

Verabschiedet am 18. März 2010

„Die bisher in der **Anlage zu § 9 BDSG** beschriebenen Maßnahmen zur Gewährleistung des technischen und organisatorischen Datenschutzes („10 Gebote“) **sind durch die Definition elementarer Schutzziele zu ersetzen**. (…)

Entsprechend den genannten Anforderungen sind folgende Schutzziele aufzunehmen:

- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Transparenz
- Nichtverkettbarkeit (als technische Sicherung der Zweckbindung)
- Intervenierbarkeit (als technische Gestaltung von Verfahren zur Ausübung der Betroffenenrechte).“

SDM
Standard-Datenschutzmodell

Um 2010 gab es weitere Entwicklungen…

- Große Organisationen nutzen zunehmend IT-Grundschutz oder haben ein Sicherheitsmanagement mit IT-SiBe, vielfach im Kontext von ITIL aufgebaut. Folge: **Die IT-Sicherheit**, die anders als Datenschutz keine eigenen normativen Grundlagen aufweisen kann, **verselbständigt sich von der normativen Führung durch Datenschutzrecht** aufgrund überzeugender Methodik.
- Bei Datenschutzprüfungen bekommt man Dokumentationen zur IT-Sicherheit aus dem GS-Tool vorgelegt mit der Behauptung, „das deckt auch die datenschutzrechtlichen Anforderungen ab!“
- **IT-Sicherheit und Datenschutz stehen vielfach in einem Konflikt**: Es zeigt sich: Auch IT-Grundschutz und IT-Sicherheitsmanagement-system (ISMS nach ISO27001) sind grundrechtskonform zu gestalten!

SDM
Standard-Datenschutzmodell

Und? Wie nun weiter?

- Wie lassen sich die Schutzziele möglichst standardisiert für Anforderungen des Datenschutzrechts operationalisieren?
- Als methodisches Vorbild gilt der erfolgreiche „IT-Grundschutz“ des BSI. Dieser weist zu jedem der (drei) Schutzziele konkrete Schutzmaßnahmen auf, die checklistenartig überprüfbar sind.

SDM
Standard-Datenschutzmodell

Bestandsaufnahme (2012)

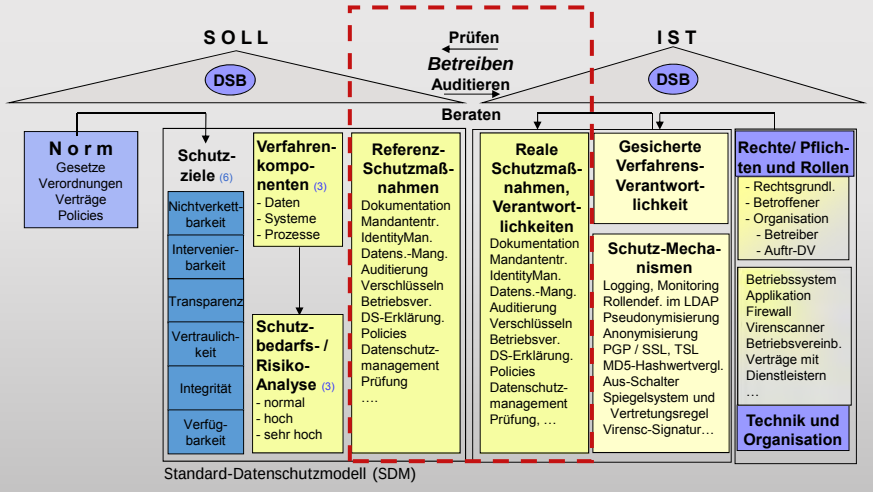
Was müssen wir DatenschützerInnen methodisch leisten?

- Wir müssen **sechs elementare Schutzziele** heranziehen, um den normativen Gehalt des Datenschutzrechts vollständig aufzunehmen, sobald eine gültige Rechtsgrundlage vorliegt.
- Aus der Prüf- und Beratungspraxis sind eine ganze Reihe an **Schutzmaßnahmen** wie Dokumentation und Protokollierung, Verschlüsselung und Signaturen, Prozesssteuerung, Regelwerke, Rollen- und Rechtekonzepte, Pseudonymisierung und Anonymisierung bekannt.
- Es hat sich gezeigt, dass **Schutzbedarfsabstufungen** für die Beurteilung der Angemessenheit und Erforderlichkeit von Schutzmaßnahmen nutzbar sind.
- Es ist sinnvoll, bei Verfahren **Datenbestände, IT-Systeme und Prozesse** zu unterscheiden, wenn man funktionale Sachverhalte prüft oder berät.

SDM
Standard-Datenschutzmodell

Standard-Datenschutzmodell „SDM“ (2012)

(Stand: 2012/06)



Standard-Datenschutzmodell (SDM)

Bock, Kirsten; Meissner, Sebastian; 2012: **Datenschutz-Schutzziele im Recht** - Zum normativen Gehalt der Datenschutz-Schutzziele; in: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 425-431.

Probst, Thomas, 2012: **Generische Schutzmaßnahmen für Datenschutz-Schutzziele**; in: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 439-444.

Martin Rost: **Standardisierte Datenschutzmodellierung**; in: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 433-438.

SDM
Standard-Datenschutzmodell

LDSG Schleswig-Holstein bekommt vollständigen Satz der sechs elementaren Schutzziele mit dem Wortlaut des „Magdeburger Treffens“ (2012)*

„(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz im Sinne von § 3 Abs. 3 ist durch technische und organisatorische Maßnahmen sicherzustellen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. Sie müssen gewährleisten, dass

- Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können **(Verfügbarkeit),**
- Daten unversehrt, vollständig, zurechenbar und aktuell bleiben **(Integrität),**
- nur befugt auf Verfahren und Daten zugegriffen werden kann **(Vertraulichkeit),**
- die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann **(Transparenz),**
- personenbezogene Daten nicht oder nur mit unverhältnismäßig hohemAufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können **(Nicht-Verkettbarkeit)** und
- Verfahren so gestaltet werden, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte nach den §§ 26 bis 30 wirksam ermöglichen **(Intervenierbarkeit)**.“

AK-Technik und DSB-Konferenz (2013)

- Das SDM wird dem AK-Technik (Sitzung 02.2013) vorgestellt
  - Zustimmung: Wir brauchen dringend eine spezifische Methodik für Datenschutzprüfungen und -beratungen.
  - Zustimmung: Die „Emanzipation von IT-Grundschutz“ ist notwendig.
  - Kritik: Datensparsamkeit soll dem Schutzziel Nicht-Verkettbarkeit nicht untergeordnet werden.
  - Empfehlung: Das Modell muss dringlich die Europa-Perspektive („EU-Grundverordnung“) aufnehmen.
  - Beschluss: Das SDM soll den Segen der DSK suchen.
  - Beschluss: Unterarbeitsgruppe SDM (UAGSDM) wird gebildet und „interdisziplinär“ besetzt.
- 85. DSK (03.2013) nimmt das SDM zur Kenntnis und erteilt den Auftrag zur Weiterentwicklung. Insbesondere wird noch eine verbesserte Ausarbeitung des Nachweises der rechtlichen Deckung der Schutzziele verlangt.

Vermittlung durch Schutzziele und SDM*

Schutzziele und deren Umsetzung durch das SDM kann außerdem wissenschaftlich untersucht und, vermittelt über Maßnahmen, auch betriebswirtschaftlich kalkuliert werden.

Martin Rost:
Zur Konditionierung von Technik und Recht,
Tagungsband der GI 2013/09

Diskussionen in der UAG (2013/2014)

Diskussionen innerhalb der UAGSDM führen zu folgenden Entscheidungen und Aktivitäten:

- „Datensparsamkeit“ wird als eigenständiges **Superschutzziel** vor die sechs elementaren Schutzziele gezogen.
- Schutzziele werden in **Gewährleistungsziele** umbenannt, um gegenüber den Ländern, deren Datenschutzgesetze bereits Schutzziele ausweisen, keine Rechtsschöpfung zu begehen.
- Entwicklung des **SDM-Handbuch**es, aus dem drei Aspekte hervorzuheben sind:
  1. Zuordnungstabell zum Nachweis der Vereinbarkeit der Schutzziele mit dem BDSG und den LDSGen (drei Typen werden unterschieden).
  2. „Ablaufmodell“ und „Strukturmodell“
  3. Betriebskonzept zur Fortschreibung des SDM

SDM-Handbuch: Mapping SZ–BDSG/LDSG

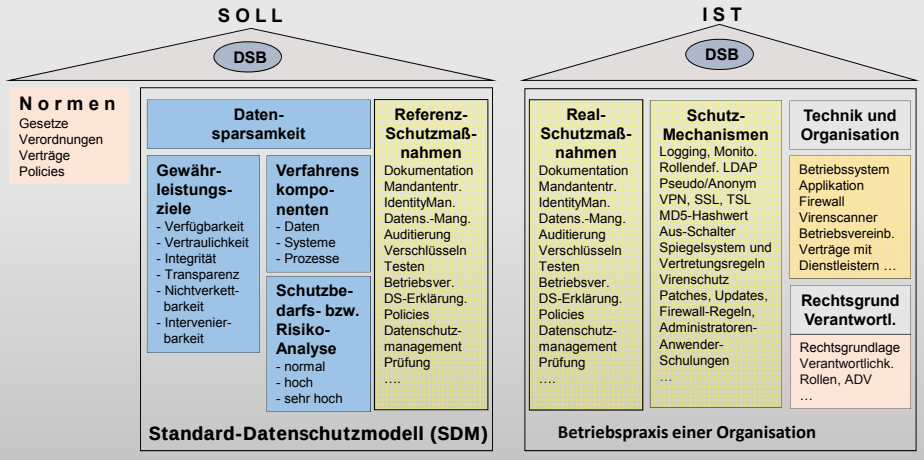
Tabelle: Zuordnung der gesetzlichen Vorgaben zu den Gewährleistungszielen.

Datensparsamkeit	Verfügbarkeit	Integrität	Vertraulichkeit	Nichtverkettbarkeit	Transparenz	Intervenierbarkeit
	Nr. 7 der Anlage zu § 9	Nr. 1-6 der Anlage zu § 9	Nr. 1-6 sowie Satz 2 der Anlage zu § 9	Nr. 8 der Anlage zu § 9		
§ 3a				§ 4 Abs. 3 Nr. 2	§ 4 Abs. 3	§ 4 Abs. 1
§ 4 Abs. 2 Nr. 2a				§ 4a Abs. 1 Satz 2	§ 4a Abs. 1 Satz 2-4, Abs. 2 Satz 2, Abs. 3	§ 4c Abs. 1 Satz 1 Nr. 1
§ 6b Abs. 3, 5				§ 4b Abs. 6	§ 4d Abs. 1 Satz 1, § 4d Abs. 5	§ 6 Abs. 1, § 6 Abs. 2 Satz 1

Aus: SDM-Handbuch, V 0.8, Seite 14f

SDM
Standard-Datenschutzmodell

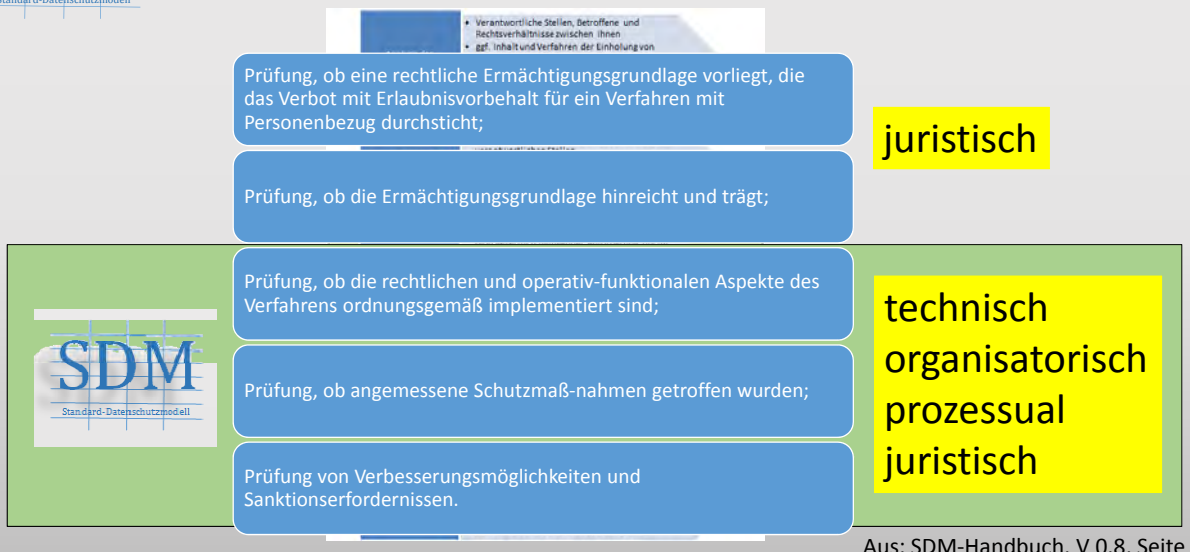
SDM-Handbuch: Prüfstruktur



Aus: SDM-Handbuch, V 0.8, Seite 31

SDM
Standard-Datenschutzmodell

SDM-Handbuch: Ablaufmodell



Aus: SDM-Handbuch, V 0.8, Seite 25

SDM-Handbuch: Betriebskonzept

- Zweck: Kontrollierte Änderung/Fortschreibung des Modells
- Eigentümerin: DSB-Konferenz
- Entwicklung und Pflege: AK-Technik
  - Bearbeitung des SDM-Handbuchs einschl. Referenz-Schutzmaßnahmen;
  - Bearbeitung von Änderungsanträgen (Change-Requests, CRs) zum SDM;
  - Sicherung der Qualität von Arbeitsergebnissen;
  - Versionierung des SDM-Handbuchs;
  - Projektmanagement, das umfasst:
    - Bereitstellung eines Single Point of Contact (Service Desk) für Beratungen und CRs;
    - Betrieb von CR-Verfolgung;
    - Moderation von Diskussionen;
    - Verwaltung der nötigen Betriebsmittel (Webseite, Projektplattform);
  - Öffentlichkeitsarbeit.

DSB-Konferenz 2014

- Das SDM-Handbuch (in der Version 0.8) wurde im Oktober 2014 von der DSK abgenommen.
- Die DSK erteilt zwei Aufträge und eine Anweisung an die UAGSDM des AK-Technik:
  - Auftrag 1: **Englisch-Übersetzung des Handbuchs,** vornehmlich mit Bezug zu Europa (Art. 29-Gruppe)
  - Auftrag 2: Entwicklung eines **Referenzkatalogs** für Standard-Maßnahmen bis zur DSK-Herbstsitzung 2015
  - Anweisung: Das SDM-Handbuch darf nur als **internes Arbeitspapier** Verwendung finden.

EU-Grundverordnung?

Das an **Grundrechten orientierte SDM steht in Konkurrenz zum stark amerikanisch beeinflussten „risk-based-approach“** (rba), der in Arbeitskreisen auf EU-Ebene eine zunehmende Rolle spielt.

ENISA (europäische Schwesterorganisation zum BSI) und die CNIL (französische Datenschutzaufsicht) unterstützen offenbar den rba. Unklar ist, welchen Einfluss der rba auf die Entwicklung der EU-Datenschutzverordnung nimmt. Es besteht das Risiko, dass Datenschutz die grundrechtliche Orientierung verliert, die auf eine Machtasymmetrie zwischen Organisationen und Personen abstellt, wenn Datenschutz zu einem privaten Risikomanagement von Einzelpersonen umdefiniert wird.

2014 / 2015: Arbeit mit/am Modell

- **Nutzung** Schutzziele / SDM
  AAL-Studie (ULD 2011), SDM: OH Smart Metering (Federführung: BfDI, Juni 2012), Cyberphysical Systems (Thiel/Hansen, DuD 2012/01) Cloud-Opinion der Art. 29-Gruppe (01037/12/EN WP196, 2012/07), PIA (Rost/Bock, DuD 2012/10), Spezifikation XTA 2.0 (XÖV-Standard OSCI-Transport, noch in Entwicklung), bei einigen KollegInnen Grundlage für Prüfungen und Beratungen
- Intensive Arbeit der UAGSDM am Katalog zu **Referenz-Schutzmaßnahmen**
- Weitere strukturell bedeutsame Entscheidungen der UAGSDM
  - Ausweis von **Standard-TO-Maßnahmen** nur für den Schutzbedarf „normal“ und „hoch“, für Schutzbedarf „sehr hoch“ sind keine Standards vorgesehen.
  - Unterscheidung nun von vier Verfahrenskomponenten:
    - Daten
    - IT-Systeme (Hardware und Software)
    - Organisatorische Prozesse (sozial-funktionale (Regelungen) von Abläufen)
    - Technische Prozesse (technisch-funktionale Abläufe)
  - Den Bezug zum IT-Grundschutz-Maßnahmenkatalog erhalten, unter Berücksichtigung der Betroffenenperspektive.

Aktuelle Kontextierungen des Modells

- Das SDM-Handbuch (V0.8) darf gemäß DSB-Konferenz-Beschluss zumindest an **externe Experten** zwecks Kommentierung herausgegeben werden.
- Zuspruch für die Verwendung des Modells unter den KollegInnen suchen. Der AK-Technik-Vorsitzende initiiert im April 2015 einen **Workshop** zum SDM mit dem Schwerpunkt *„juristische Problemstellungen“*.
- Erste **SDM-Schulungen** werden durchgeführt (Datenschutzakademie Leck).

Die nächsten Schritte… (2015)

- Weiterarbeit an der Erstellung des Referenzmaßnahmenkatalogs
  - Nächste Sitzung: 16. Juni 2015, Berlin
  - Ziel: Entwurf eines Maßnahmenkatalogs für den AK-Technik bzw. die DSB-Konferenz im Herbst 2015
- Überarbeitung des Handbuches (V0.8) anhand bislang eingetroffener Kommentare und Änderungswünsche
- Kontakt nach Brüssel (Art. 29, ENISA, CNIL) suchen (BfDI)
- Kontakt zu Normierungsinstanzen suchen: DIN, ISO, Gremien des IT-Planungsrats

SDM
Standard-Datenschutzmodell

Vielen Dank für Ihre Aufmerksamkeit.

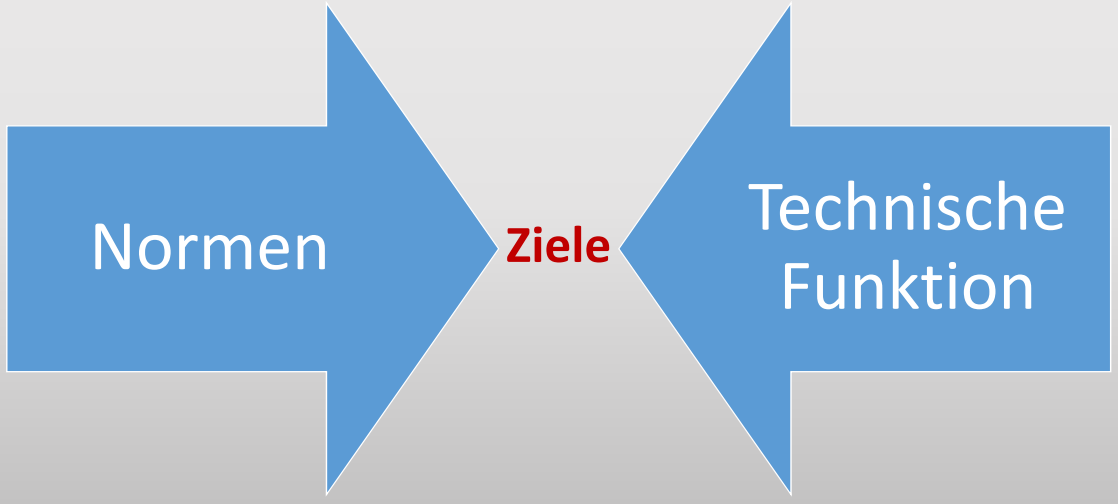
Martin Rost

Unabhängiges Landeszentrumfür
Datenschutz Schleswig-Holstein
Holstenstraße 98, 24103 Kiel
Tel.: 0431-988 1200
www.datenschutzzentrum.de
ULD: mail@datenschutzzentrum.de
persönlich: martin.rost@datenschutzzentrum.de

Das BDSG als Basis für das Standard-Datenschutzmodell

Meike Kamp
Berliner Beauftragter für Datenschutz und Informationsfreiheit

Gewährleistungsziele



Gewährleistungsziele – wofür?

- Wie kann der Jurist sichergehen, dass rechtliche Anforderungen tatsächlich technisch umgesetzt werden?
- Normen lassen sich nicht ohne Weiteres technisch operationalisieren, d. h. in technische Funktionen umsetzen.

➔ **Lösung: Gemeinsame Sprache finden!**

- Was soll die Norm bewirken? ➔ Zuordnung zu den Zielen
- Ziel ➔ Technische Funktion zur Erreichung des Ziels.

Woher kommen die Gewährleistungsziele?

- Gewährleistungsziele entsprechen den Kernforderungen zur Absicherung des Rechts auf informationelle Selbstbestimmung
  - z.B. BVerfG 65, 1: Keine unbegrenzte Erhebung und Verarbeitung, Schutz vor Verknüpfungsmöglichkeiten/Zweckentfremdung, Selbstbestimmung, Überschaubarkeit der über sich selbst bekannten Informationen etc.
- Datenschutzrechtliche Anforderungen können entsprechend ihrem Gehalt und ihrer Zielrichtung strukturiert unter die Gewährleistungsziele zusammengefasst werden.

SDM
Standard-Datenschutzmodell

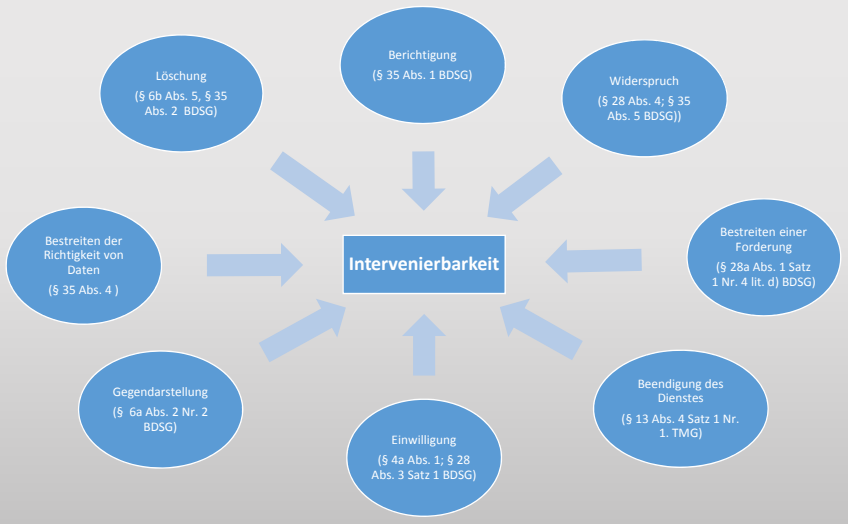
Gesetzliche Verankerung

- Datenschutzrechtliche Anforderungen können über die Gewährleistungsziele in erforderliche technische und organisatorische Maßnahmen transformiert werden.
- Gewährleistungsziele beinhalten ausschließlich Forderungen, die gesetzlich gedeckt sind.

➔ Gewährleistungsziele sind gesetzlich verankert!

SDM
Standard-Datenschutzmodell

Beispiel: Intervenierbarkeit



SDM
Standard-Datenschutzmodell

„BDSG-Mapping“

Daten-sparsamkeit	Verfügbarkeit	Integrität	Vertraulichkeit	Nichtverkett-barkeit	Transparenz	Intervenier-barkeit
§ 3a	§ 9 i. V. m. Nr. 7 der Anlage	§ 6c Abs. 1 Nr. 4	§ 5	§ 4 Abs. 3 Nr. 2	§ 4 Abs. 3	§ 4 Abs. 2
§ 4c Abs. 1 Satz 1 Nr. 2, 3, 4, 5	§ 34 Abs. 2 Satz 1 Nr. 1	§ 9 i. v. m. Nr. 1-6 der Anlage	§ 4f Abs. 4	§ 4a Abs. 1 Satz 2	§ 4a Abs. 1 Satz 2	§ 4a
§§ 6, 6b Abs. 1	§ 35 Abs. 3 Nr. 2	§ 35 Abs. 1	§ 9 i. V. m. Nr. 1-6 der Anlage	§ 4c Abs. 1 Nr. 2, 3, 4	§§ 6 Abs. 1, 33, 34	§ 6a
…	…	…	…	…	…	…

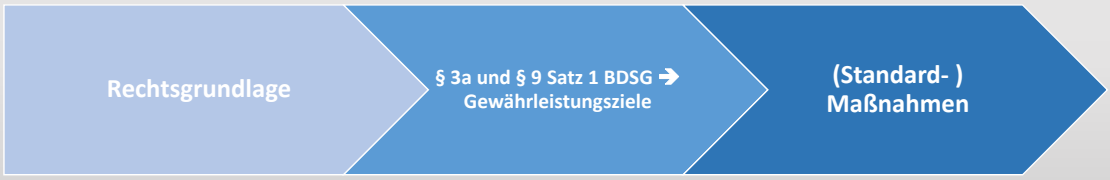
AK Technik-Workshop 2015
Hannover, 29.04.2015

„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen

7

SDM
Standard-Datenschutzmodell

Operationalisierung datenschutzrechtlicher Anforderungen



AK Technik-Workshop 2015
Hannover, 29.04.2015

„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen

8

Gesetzliche Verortung der Operationalisierung

- *§ 3a Satz 1 BDSG: „… Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, … “*
- § 9 Satz 1 BDSG: *„… die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, … , zu gewährleisten.“ (§ 9 Satz 1 BDSG)*

Pflicht zur Vermeidung von Rechtsverstößen

- **Volkszählungsurteil BVerfGE 65, 1:** *„Auch hat er [der Gesetzgeber] organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.“*
- **Erwägungsgrund 46 der RL 95/46/EG**: *„Für den Schutz der Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung personenbezogener Daten müssen geeignete technische und organisatorische Maßnahmen getroffen werden, und zwar sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt der eigentlichen Verarbeitung, um insbesondere deren Sicherheit zu gewährleisten und somit jede unrechtmäßige Verarbeitung zu verhindern.“*

Pflicht zur Vermeidung von Rechtsverstößen

- Verbot mit Erlaubnisvorbehalt, § 4 Abs. 1 BDSG
  - ➔Beweislast auf Seiten der verantwortlichen Stelle
  - ➔Die verantwortliche Stelle muss vor der Datenverarbeitung wissen, ob diese zulässig ist.
- Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel der Datensparsamkeit auszurichten, § 3a Satz 1 BDSG
- Maßnahmen zur Gewährleistung der Ausführung der Vorschriften des BDSG, § 9 Satz 1 BDSG
  - ➔ Nur wenn der ordnungsgemäße Umgang mit einem Ereignis vorab festgelegt und abgesichert wurde, kann für den Zeitpunkt des Eintritts des Ereignisses gewährleistet werden, dass die datenschutzrechtlichen Anforderungen eingehalten werden.

Vielen Dank!

Meike Kamp
Berliner Beauftragter für Datenschutz und Informationsfreiheit
kamp@datenschutz-berlin.de
030 / 13889-314

Verankerung der Gewährleistungsziele in den Landesdatenschutzgesetzen

Dr. Tino Naumann
Leiter Geschäftsstelle
Sächsischer Datenschutzbeauftragter

- Etliche Landesdatenschutzgesetze sehen wie das BDSG bestimmte Kontrollen vor (HB, Hessen, RLP, Saarland, BY, BW und Niedersachsen):
  - Zugangskontrolle,
  - Datenträgerkontrolle,
  - Speicherkontrolle,
  - Benutzerkontrolle,
  - Zugriffskontrolle,
  - Übermittlungskontrolle,
  - Eingabekontrolle,
  - Auftragskontrolle,
  - Transportkontrolle,
  - Organisationskontrolle

SDM
Standard-Datenschutzmodell

- 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 von Berlin, Hamburg und Nordrhein-Westfalen enthalten die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit sowie Transparenz (mit Ausnahme von Hamburg), Authentizität und Revisionsfähigkeit.
- Das Landesdatenschutzgesetz von Schleswig-Holstein enthält seit Januar 2012 sämtliche Gewährleistungsziele, wobei Datensparsamkeit nicht als Schutzziel aufgeführt ist, sondern separat vorgeschrieben ist

SDM
Standard-Datenschutzmodell

- 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 (Sachsen) 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“ nicht bereits in bestehenden Schutzzielen verankert.

Herleitung der Gewährleistungsziele aus dem SächsDSG

Datensparsamkeit	Verfügbarkeit	Integrität	Vertraulichkeit	Nichtverkettbarkeit	Transparenz	Intervenierbarkeit
§ 9 Abs. 1 Satz 2	§ 9 Abs. 2 Nr. 3	§ 9 Abs. 2 Nr. 2	§ 9 Abs. 2 Nr. 1		§ 9 Abs. 2 Nrn. 4-6	
§§ 20, 21 Abs. 2 Satz 2 (Löschung /Sperrung bei entfallener Erforderlichkeit)				§ 4 Abs. 3 (Zweckfestlegung bei Einwilligung)	§ 4 Abs. 3 (informierte Einwilligung)	§ 4 Abs. 1 Nr. 2 (Einwilligung/Rücknahme)
§ 36 Abs. 2 (Pseudonymisierung /Anonymisierung bei wiss. Forschung)				§ 10 Abs. 1 Nr. 2 (Zweckbestimmung im Verfahrens-verzeichnis)	§3 10, 11 Abs. 4 Nr. 5, 31 Abs. 2 (Verfahrensverzeichnis)	§§ 19-22 (Berichtigung, Löschung, Sperrung, Widerspruch)
§ 33 Abs. 4 (Löschfrist bei Videoaufzeichnungen)				§ 12 Abs. 2, 5, 6 (Zweckfestleung bei Erhebung)	§ 12 (Informationspflichten bei Datenerhebung)	§ 32 Abs. 1 (Fernmessen und Fernwirken)

SDM
Standard-Datenschutzmodell

Herleitung der Gewährleistungsziele aus dem SächsDSG

Datensparsamkeit	Verfügbarkeit	Integrität	Vertraulichkeit	Nichtverkettbarkeit	Transparenz	Intervenierbarkeit
§ 12 (Erhebung nur bei Erforderlichkeit)				§ 13 (Zweckbindung bei Speicherung etc.)	§§ 18, 34 Abs. 3 (Auskunft/Einsicht)	
§ 13 (Speicherung etc. nur bei Erforderlichkeit)				§§ 14 Abs. 3, 16 Abs. 4 (Zweckbindung bei Übermittlung)	§ 27 (Kontrolle ducrh SächsDSB)	
§§ 14, 15, 16, 17 (Übermittlung nur bei Erorderlichkeit)				§ 32 Abs. 1 (Zweckbindung bei Fernmessen und Fernwirken)	§ 32 (Informationspflicht bei Fernmessen und Fernwirken)	
				§ 33 (Zweckbindung Video)	§ 33 Abs. 3 (Videoüberwachnung)	
				§ 34 (automatisierte Einzelentscheidung)	§ 35 Abs. 2 (mobile Medien)	

AK Technik-Workshop 2015
Hannover, 29.04.2015

„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen

7

Der europäische Bezug des Standard-Datenschutzmodells

AK Technik-Workshop 2015
Kirsten Bock

Geschichte ab 1970

- Europäische Gesetzgeber konnten kaum auf Erfahrung und Gerichtsentscheidungen zur automatisierten Datenverarbeitung zurückgreifen

  Folge: Herantasten durch
  - Generalklauseln (Hessen HDSG 1970)
  - Genehmigungspflicht (Schweden 1973)
    - Offenlegung der Verarbeitungsziele und –modalitäten gegenüber einer Kontrollinstanz
    - Korrigiert den „lückenhaften Wissenstand des Gesetzgebers“ (Simitis)
  - Sektorspezifische Regelungen (USA, Fair Credit Reporting Act 1970)

Geschichte ab 1980

- Scheitern der Regelungsvorstellungen
  - Genehmigungs- und Lizensierungsmodell: übermäßige Bürokratie bei stark wachsender Automatisierung der DV
  - Versagen des Generalklauseln: übermäßig interpretationsoffen, interessengeleitet
  - Bereichsspezifische Regelungen: begrenzte Regelungsgegenstände führen zu zerfaserten, unterschiedlichen Regelungen, die eine systematische Überprüfung verschiedener Verarbeitungsbereiche erschweren
- DSG Niederlande (1988): typische Mischung von Genehmigungs-pflicht und allgemeinen Verarbeitungsgrundsätzen entwickelt sich zur Frage nach der **Wirksamkeit normativer Anforderungen** und Regulierung einzelner Verarbeitungssituationen.

Verträge und Rechtsakte

- Konvention 108 des Europarats (1981) (optional)
  - Machte aus partikulären, nationalen Grundsätzen international akzeptierte Verhaltensregeln: 5 Verarbeitungsgrundsätze + Betroffenenrechte + sensitive Daten
- EG-Datenschutzrichtlinie 95/46/EG (verbindlich)
  - Übermittlung nur in Drittstaaten mit „angemessenem Datenschutzniveau", Art. 25 Abs. 1, befördert die Angleichung der Regelungen

  ➢Fokussierung auf das (Schutz-) Ziel
- EU Grundrecht: Charta der EU (2000)
  - Grundrecht auf Datenschutz, Art. 8
  - Verbindlich durch Art. 6 Abs. EUV (Vertrag von Lissabon 2007)

SDM
Standard-Datenschutzmodell

Weiterentwicklung des DSR in Europa

- Zunahme informationstechnischer Möglichkeiten verursacht Schutzlücken
  - Überarbeitung der Europäischen Datenschutzkonvention 108 (nicht verabschiedet)
  - Entwurf einer Datenschutzgrundverordnung (DSG-VO), 2012
- Problem: Wirksamkeit des Datenschutzes hängt von der Fähigkeit des Rechts ab, gezielt aus der Perspektive der Betroffenen auf wichtige Verarbeitungssituationen zu reagieren, um die informationellen Grundrechte zu gewährleisten.

SDM
Standard-Datenschutzmodell

Lösungsansätze in der Diskussion

- Bereichsspezifische Konkretisierungen
  - technologieabhängig
  - uneinheitlich
- Risikoansatz (RBA)
  - Abkehr vom Zweckbindungsgrundsatz
  - Schadensermittlung statt Grundrechtsgewährleistung
  - unbestimmt
- Selbstregulierung
  - interessengeleitet, dadurch nicht zielführend ausgerichtet am Grundrechtsschutz der Betroffenen
- Gewährleistungsziele
  - grundrechtefokussiert
  - technologieneutral
  - konkret und flexibel in den Maßnahmen

Gewährleistungsziele im EU Datenschutzrecht

- Datenschutzrechtliche Anforderungen können über die Gewährleistungsziele in erforderliche technische und organisatorische Maßnahmen transformiert werden.
- Gewährleistungsziele beinhalten keine Forderungen, die nicht vom EU-Recht gedeckt sind.

➔ Gesetzliche Verankerung der Gewährleistungsziele

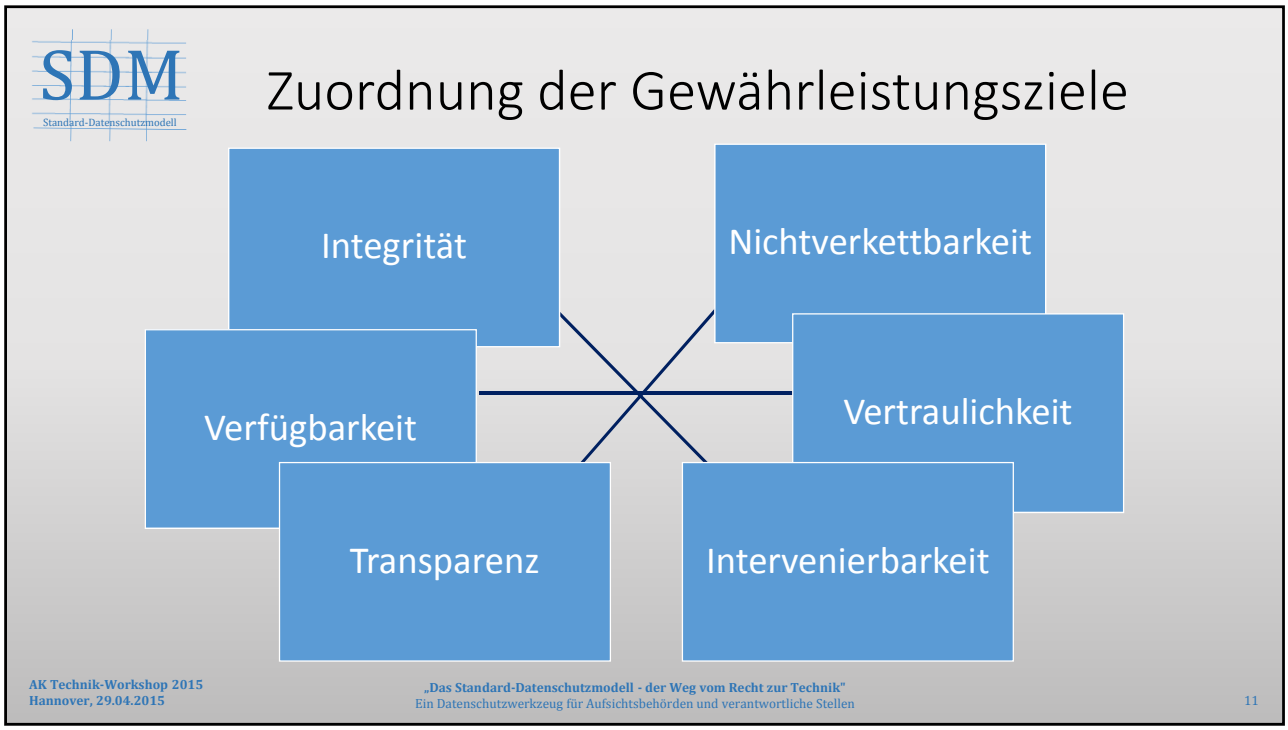
Art. 8 EU Charta Art. 1 I RL 95/46/EG	• Grundrechtsschutz: Gewährleistung der informationellen Grundrechte
Art. 5, 7 DSRL	• Grundsätze der Rechtmäßigkeit der Verarbeitung personenbezogener Daten • Rechtsgrundlage • Zwecksetzung und Zweckbindung • Datensparsamkeit
Art. 17 I DSRL	• Vertraulichkeit und Sicherheit der Verarbeitung • Strukturierung und Festlegung der "erforderlichen" technischen und organisatorischen Maßnahmen • Unterstützung des juristischen Abwägungsprozesses

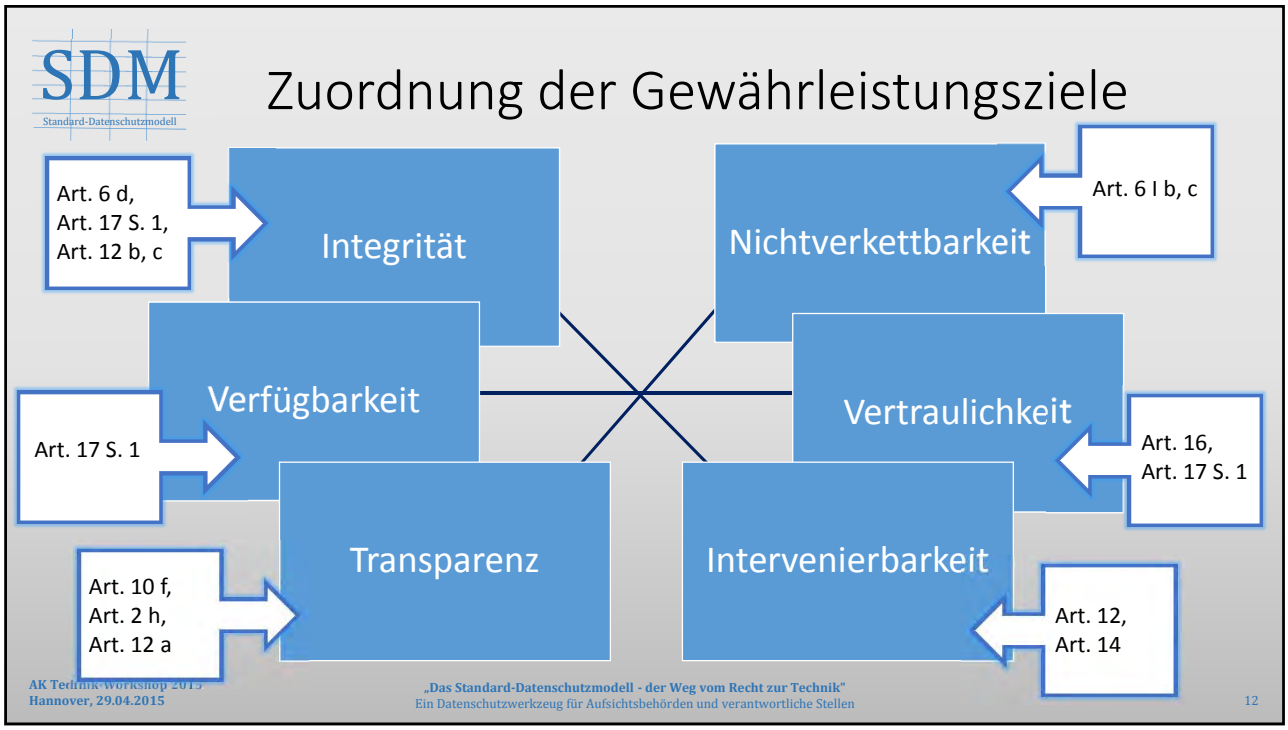
Art. 17 Abs. 1 DSRL

- „Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche die **geeigneten technischen und organisatorischen Maßnahmen** durchführen muss, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten **erforderlich** sind.
- Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung entstehenden Kosten ein **Schutzniveau** gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten **angemessen** ist.“

Pflicht zur Vermeidung von Rechtsverstößen

- **Erwägungsgrund 46 der RL 95/46/EG**: *„Für den Schutz der Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung personenbezogener Daten müssen geeignete technische und organisatorische Maßnahmen getroffen werden, und zwar sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt der eigentlichen Verarbeitung, um insbesondere deren Sicherheit zu gewährleisten und somit jede unrechtmäßige Verarbeitung zu verhindern.“*


SDM
Standard-Datenschutzmodell
Zuordnung der Gewährleistungsziele
Integrität
Nichtverkettbarkeit
Verfügbarkeit
Vertraulichkeit
Transparenz
Intervenierbarkeit
AK Technik-Workshop 2015
Hannover, 29.04.2015
„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen
11


SDM
Standard-Datenschutzmodell
Zuordnung der Gewährleistungsziele
Art. 6 d,
Art. 17 S. 1,
Art. 12 b, c
Integrität
Art. 6 I b, c
Nichtverkettbarkeit
Verfügbarkeit
Art. 17 S. 1
Vertraulichkeit
Art. 16,
Art. 17 S. 1
Transparenz
Art. 10 f,
Art. 2 h,
Art. 12 a
Intervenierbarkeit
Art. 12,
Art. 14
AK Technik-Workshop 2015
Hannover, 29.04.2015
„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen
12

SDM
Standard-Datenschutzmodell

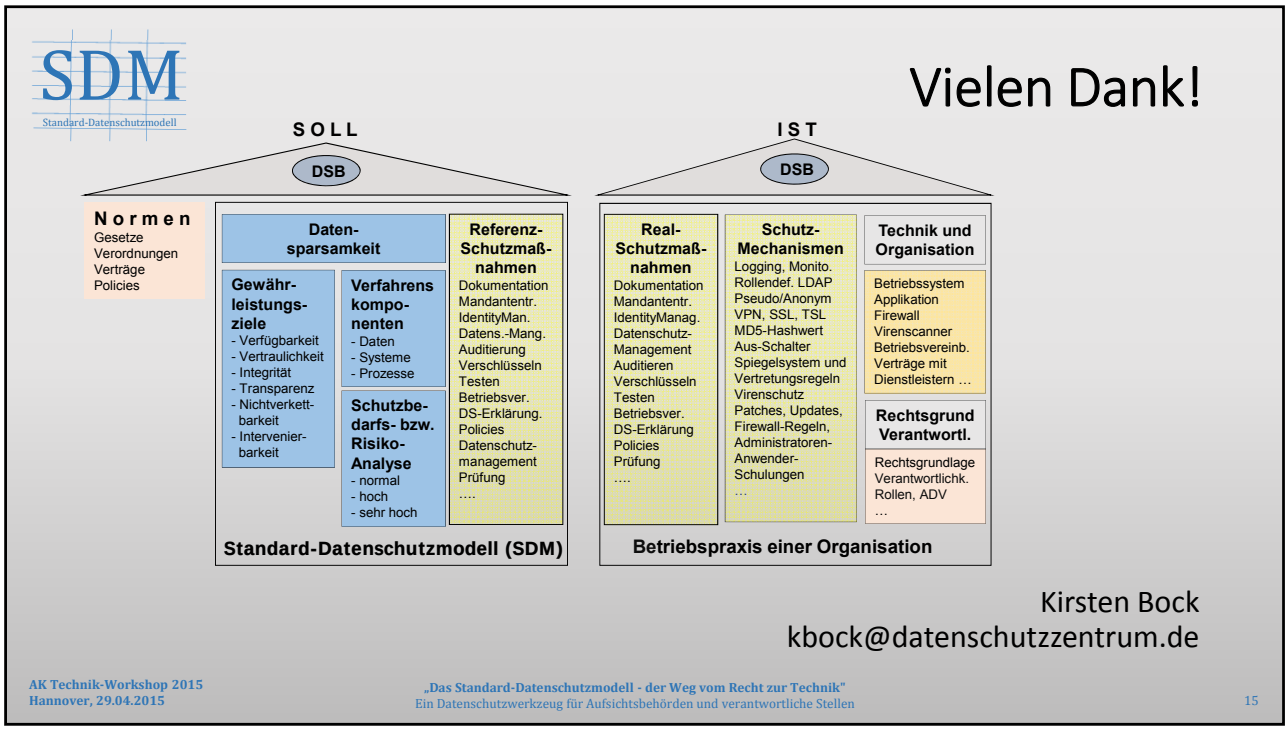
Mapping

	Datensparsamkeit	Verfügbarkeit	Integrität	Vertraulichkeit	Nichtverkettbarkeit	Transparenz	Intervenierbarkeit
RL 95/46/EG		Art. 17 S. 1	Art. 6 d), Art. 17 S. 1, Art. 12 b), c)	Art. 16, Art. 17 S. 1	Art. 6 b), c), e)	Art. 10 f), Art. 2 h), Art. 12 a)	Art. 12, Art. 14
DSGVO-E 2012 Art. 30: technische und organisatorische Maßnahmen	Art. 5 c), Art. 10	Art. 20 II	Art. 20 II	Art. 20 II	Art. 5 b, Art. 23 „PbD“	Art. 5 f), Art. 11, Art. 14, Art. 22, Art. 28, Art. 31, 32 „data breach notification“	Art. 12, Art. 15, Art. 16, Art. 17, Art. 18, Art. 19

SDM
Standard-Datenschutzmodell

Ausblick

- Bedeutung des SDM als Mittler zwischen Recht und Technik
- Stärkung des Grundrechtsansatzes gegenüber Risiko- und Schadensmodellen


SDM
Standard-Datenschutzmodell
Vielen Dank!
SOLL
DSB
Normen
Gesetze
Verordnungen
Verträge
Policies
Daten-sparsamkeit
Gewähr-leistungs-ziele
- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Transparenz
- Nichtverkett-barkeit
- Intervenier-barkeit
Verfahrens kompo-nenten
- Daten
- Systeme
- Prozesse
Schutzbe-darfs- bzw. Risiko-Analyse
- normal
- hoch
- sehr hoch
Referenz-Schutzmaß-nahmen
Dokumentation
Mandantentr.
IdentityMan.
Datens.-Mang.
Auditierung
Verschlüsseln
Testen
Betriebsver.
DS-Erklärung.
Policies
Datenschutz-management
Prüfung
....
Standard-Datenschutzmodell (SDM)
IST
DSB
Real-Schutzmaß-nahmen
Dokumentation
Mandantentr.
IdentityManag.
Datenschutz-Management
Auditieren
Verschlüsseln
Testen
Betriebsver.
DS-Erklärung
Policies
Prüfung
....
Schutz-Mechanismen
Logging, Monito.
Rollendef. LDAP
Pseudo/Anonym
VPN, SSL, TSL
MD5-Hashwert
Aus-Schalter
Spiegelsystem und
Vertretungsregeln
Virenschutz
Patches, Updates,
Firewall-Regeln,
Administratoren-
Anwender-
Schulungen
...
Technik und Organisation
Betriebssystem
Applikation
Firewall
Virenscanner
Betriebsvereinb.
Verträge mit
Dienstleistern ...
Rechtsgrund Verantwortl.
Rechtsgrundlage
Verantwortlichk.
Rollen, ADV
...
Betriebspraxis einer Organisation
Kirsten Bock
kbock@datenschutzzentrum.de
AK Technik-Workshop 2015
Hannover, 29.04.2015
„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen
15

SDM
Standard-Datenschutzmodell

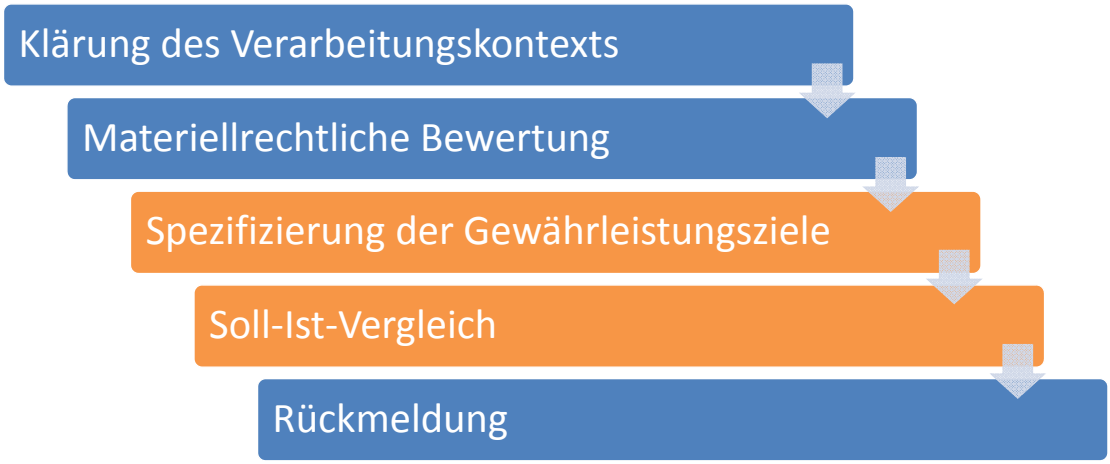
Prüfen und Beraten mit dem Standard-Datenschutz-Modell

Dr. Ulrich Vollmer

Berliner Beauftragter für Datenschutz und Informationsfreiheit
Bereich Informatik

SDM
Standard-Datenschutzmodell

Vorgehensweise



SDM
Standard-Datenschutzmodell

Verarbeitungskontext

Wer

- Verantwortliche Stellen, Betroffene, Rechtsverhältnisse

Wofür

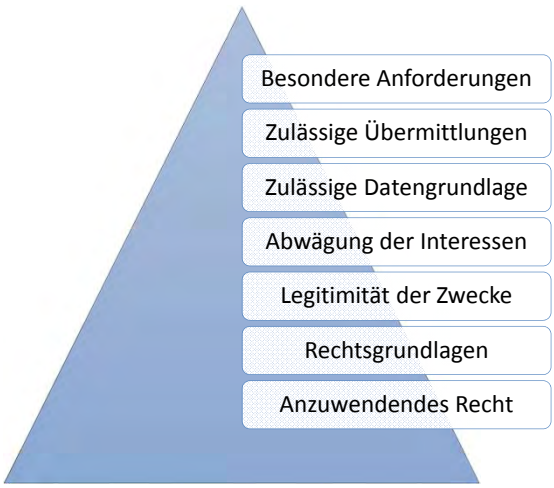
- Zwecke und Geschäftsprozesse

Was

- Datengrundlage, Datenfluss, Verarbeitungsprozess

SDM
Standard-Datenschutzmodell

Materiellrechtliche Bewertung



SDM
Standard-Datenschutzmodell

Spezifizierung der Gewährleistungsziele

Qualitative Parameter

Wer ist Berechtigt? | Welche Zwecke sind kompatibel?

Einstufung des Schutzbedarfs

Welche Folgen für Betroffene: | Selbstbestimmung, finanziell, Leib und Leben

Quantitative Parameter

Wie schnell Auskunft? | DV wie detailliert nachvollziehbar?

SDM
Standard-Datenschutzmodell

Gewährleistungsziel präzisieren

Vertraulichkeit

Wer ist befugt?

Keine unbefugte Person nimmt

personenbezogene Daten zur Kenntnis.

Auf welche Daten?

Unter welchen Bedingungen?

Aufgabe – Betroffene – Datenart

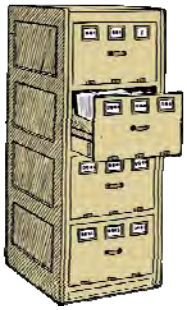
Gewährleistungsziel präzisieren

Verfügbarkeit

Welche? Für wen?

Personenbezogene Daten stehen zur Verfügung und können ordnungsgemäß im vorgesehenen Prozess verwendet werden

Welche Abweichungen sind tolerabel?



AK Technik-Workshop 2015 Hannover, 29.04.2015

„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen

Dr. Ulrich Vollmer, Berlin
7

Gewährleistungsziel präzisieren

Integrität

Interessensabwägung

Daten bleiben unversehrt, vollständig,aktuell.

Systeme bleiben spezifikationskonform.

Welche Eigenschaften

Unter welchen Bedingungen?

Störfall – Einwirkungen Unbefugter

AK Technik-Workshop 2015 Hannover, 29.04.2015

„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen

Dr. Ulrich Vollmer, Berlin
8

Gewährleistungsziel präzisieren

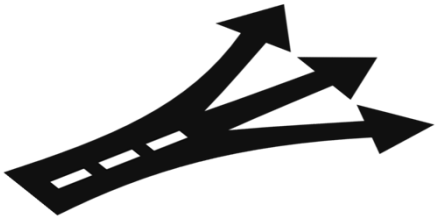
Nichtverkettung

Zulässige Zweckänderungen

welcher Angaben?

Verarbeitung nur für Zwecke,

für die die Daten erhoben wurden.



Quantifizierung

Höhe der Hürden

Bsp. Funktionstrennung

Gewährleistungsziel präzisieren

Transparenz

Art der Verarbeitung

- Welche Daten werden für welchen Zweck wie von wem
  - in IT-Anlagen gespeichert, verändert und gelöscht?
  - genutzt?
  - übermittelt? An wen?
- Welche Systeme und Prozesse werden dafür verwendet?
- Wer hat die rechtliche Verantwortung für Daten und Systeme?

Umfang und Detailtiefe der Dokumentation

Gewährleistungsziel präzisieren

Intervenierbarkeit

Technische Voraussetzungen schaffen für
- Auskunft,
- Benachrichtigung,
- Berichtigung,
- Sperrung
- Löschung

Voraussetzungen

Verpflichtung unabhängig von Eintritt der Situation

Gewährleistungsziel präzisieren

Datensparsamkeit

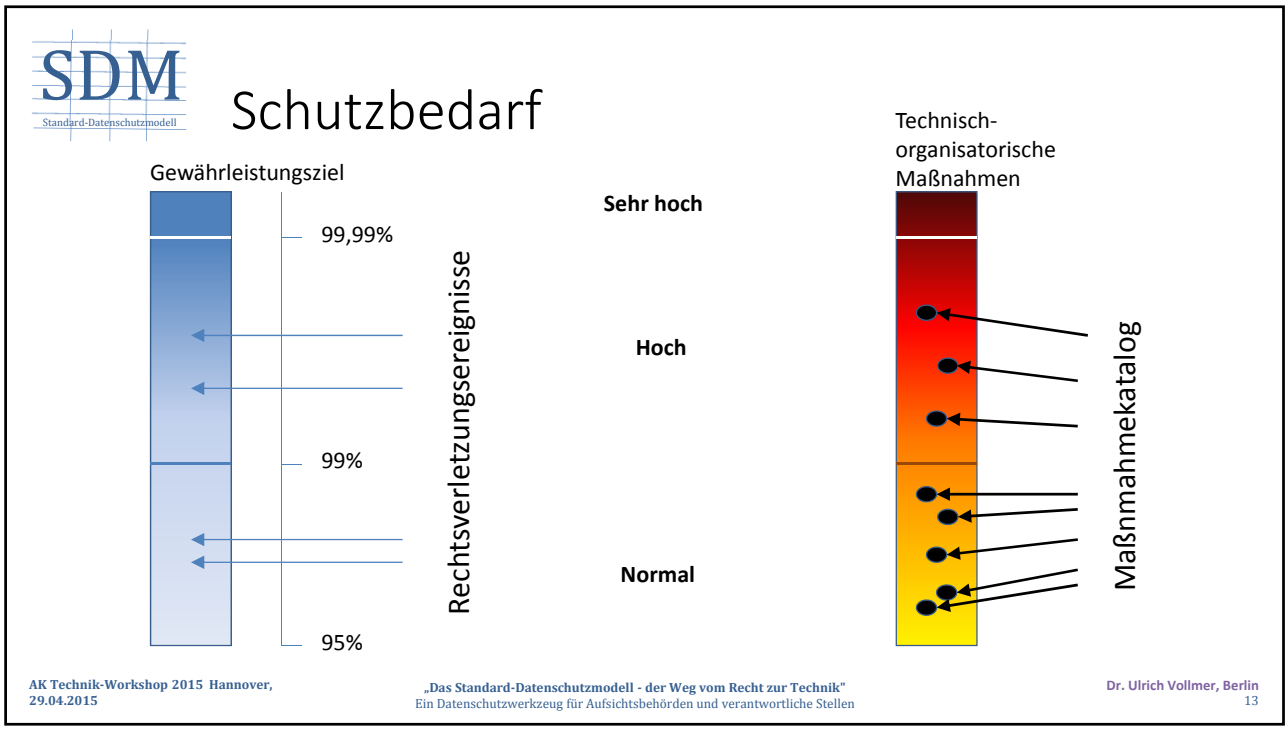
Erforderlichkeit?

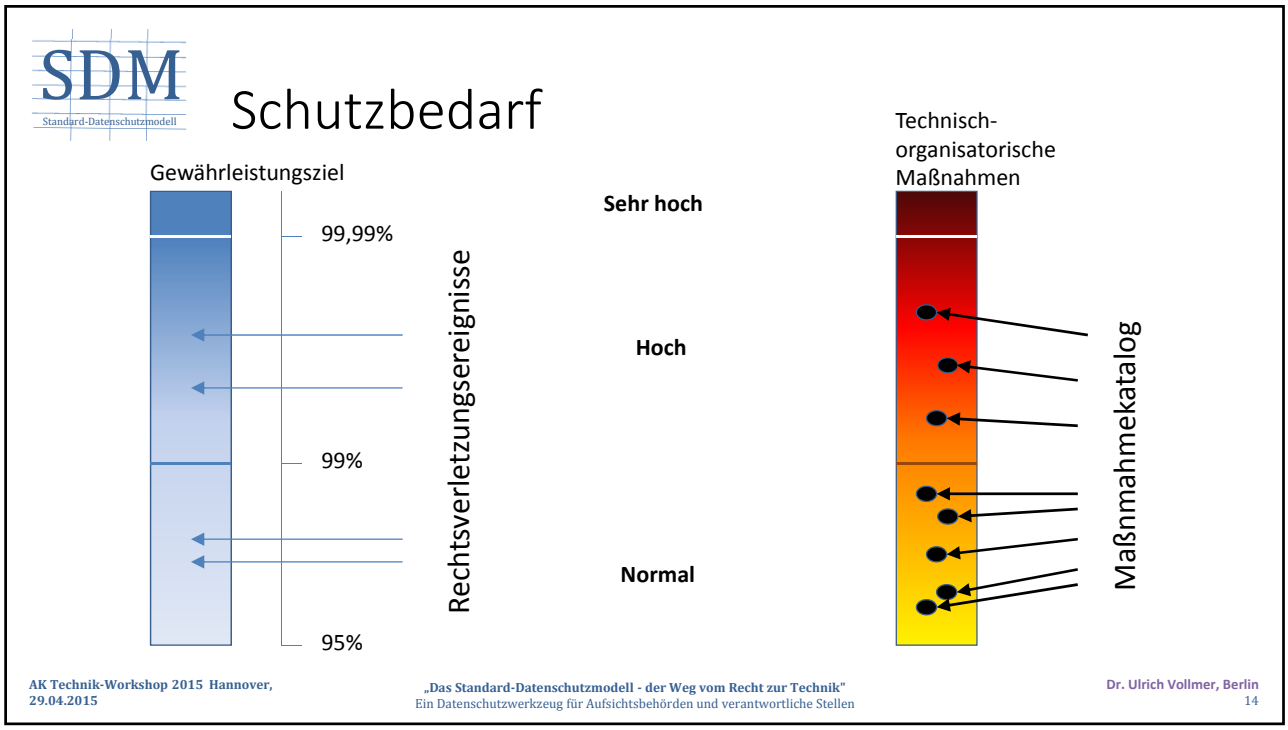
Minimiere
- Umfang der Daten, die verarbeitet und offenbart werden,
- Zahl der Stellen und Personen, an die sie offenbart werden,
- Verfügungsgewalt der zugriffsberechtigten Personen

… im gesamten Prozess
und jedem Verarbeitungsschritt

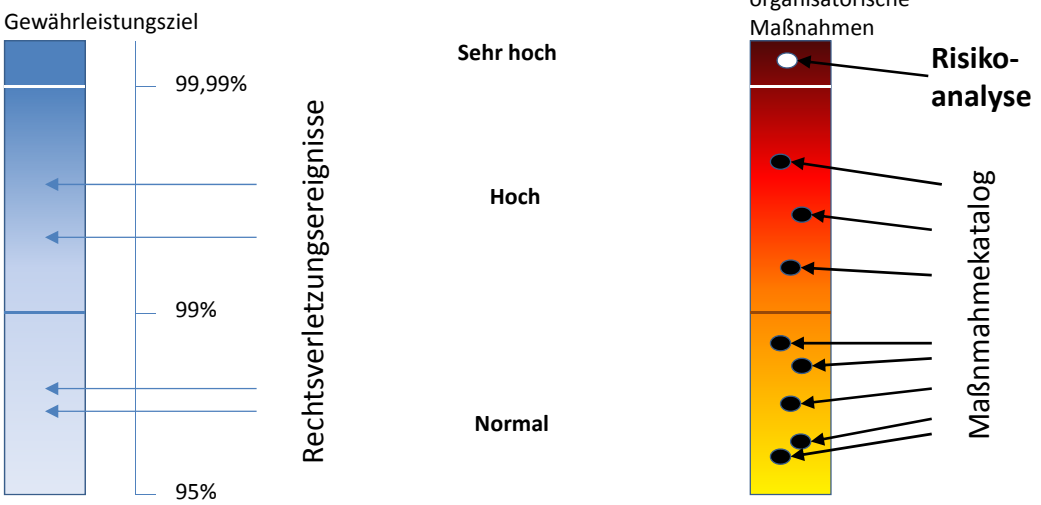
Gewicht?

Eingriffstiefe?


SDM
Standard-Datenschutzmodell
Schutzbedarf
Gewährleistungsziel
99,99%
99%
95%
Rechtsverletzungsereignisse
Sehr hoch
Hoch
Normal
Technisch-organisatorische Maßnahmen
Maßnmahmekatalog
AK Technik-Workshop 2015 Hannover, 29.04.2015
„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen
Dr. Ulrich Vollmer, Berlin
13


SDM
Standard-Datenschutzmodell
Schutzbedarf
Gewährleistungsziel
99,99%
99%
95%
Rechtsverletzungsereignisse
Sehr hoch
Hoch
Normal
Technisch-organisatorische Maßnahmen
Maßnmahmekatalog
AK Technik-Workshop 2015 Hannover, 29.04.2015
„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen
Dr. Ulrich Vollmer, Berlin
14

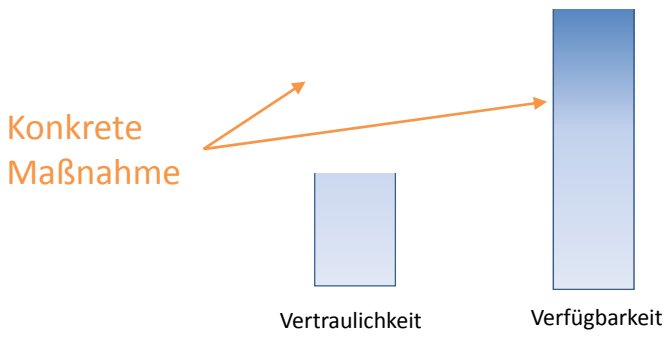
Schutzbedarf



Abwägung

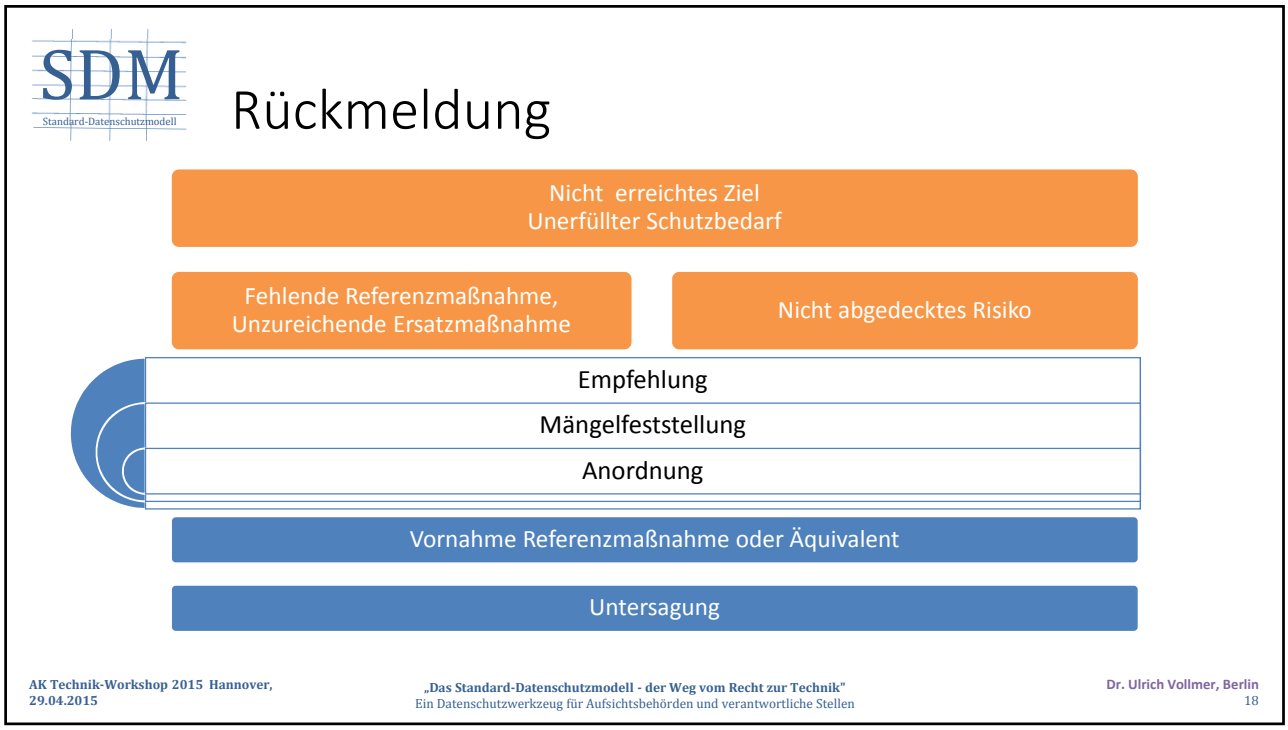
Die Gewährleistungsziele sind widerspruchsfrei.

ABER



ABWÄGUNG


SDM
Standard-Datenschutzmodell
Soll-Ist-Vergleich
Institutioneller Kontext
• Datenschutzmanagement, Verantwortung
Technischer Kontext
• Systeme, Netze, Prozesse, Personal
Technisch-organisatorische Maßnahmen
• Abgleich mit Referenzmaßnamen aus Katalog
Wirksamkeitsbetrachtung
• Äquivalente Maßnahmen, nachvollziehbare Risikoanalyse
AK Technik-Workshop 2015 Hannover, 29.04.2015
„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen
Dr. Ulrich Vollmer, Berlin
17


SDM
Standard-Datenschutzmodell
Rückmeldung
Nicht erreichtes Ziel
Unerfüllter Schutzbedarf
Fehlende Referenzmaßnahme,
Unzureichende Ersatzmaßnahme
Nicht abgedecktes Risiko
Empfehlung
Mängelfeststellung
Anordnung
Vornahme Referenzmaßnahme oder Äquivalent
Untersagung
AK Technik-Workshop 2015 Hannover, 29.04.2015
„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen
Dr. Ulrich Vollmer, Berlin
18

SDM
Standard-Datenschutzmodell

Vielen Dank für Ihre Aufmerksamkeit!

Herzliche Einladung zur Diskussion,
jetzt und nach den Fallbeispielen.

Ulrich Vollmer

Usecase aus dem öffentlichen Bereich: TKÜ-Verfahren

Michael Wilms,
Referat Technik
Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
&
Uwe Robra
Referatsleiter technisch-organisatorischer Datenschutz und bei Telemedien/Rundfunk
Die Landesbeauftragte für den Datenschutz Niedersachsen

Inhalt

- Ausgangslage/erste juristische Bewertung
- Was bedeutet TKÜ?
- Modellierung nach SDM
- Schutzbedarfsanalyse
- Überblick über die Referenzmaßnahmen
- Bespiel: Maßnahmen der Integrität

SDM
Standard-Datenschutzmodell

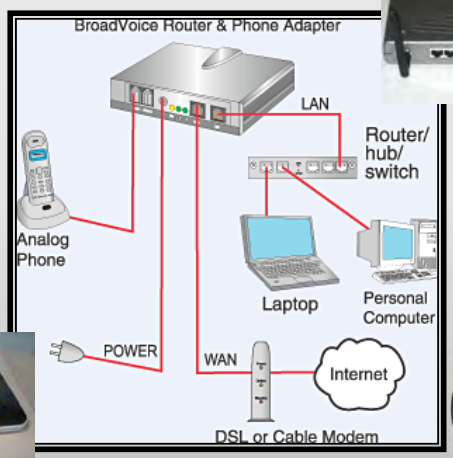
Ausgangslage/ erste juristische Bewertung

- Ermittlungsbehörden und teilweise Gefahrenabwehrbehörden führen Überwachungs-Maßnahmen im Bereich der Telekommunikation (TK) als Ultima Ratio durch (bundesweit in 2013 lt. BA für Justiz z.B. 5.669 Verfahren mit 22.917 Erst- und Verlängerungsanordnungen nach § 100a StPO)
- Zweck: Strafverfolgung und Prävention bei schweren Straftaten, z.B. BTM, OK, Drogen, Terror, Kriegswaffen, aber auch Bestechung/Bestechlichkeit
- Juristische Prüfung:
  Anlassbezogene Überwachung / präventive Überwachung (Speicherung der Daten von Unbeteiligten)
- Rechtsgrundlagen StPO: § 100a (Inhalt), § 94 (Simkarte) §§ 161 Abs. 1, 163 Abs. 1 i.V.m. § 113 TKG (Bestandsdaten), § 112 TKG (Personenauskunft)
  Einschränkung:
  - Anordnung nur gegen Beschuldigten oder bestimmte beteiligte Personen (§ 100a Abs. 3 StPO)
  - Kernbereich privater Lebensgestaltung ist tabu (§ 100a Abs. 4 StPO)
- Rechtsgrundlagen Gefahrenabwehrrecht Land: z.B. § 33 a Nds. SOG zur Gefahrenabwehr (Inhalt, Verkehrsdaten, Standortdaten) oder §§ 20a, 20b PolG NRW
- Zu beachten: TOM (z.B. § 7 NDSG, § 9 BDSG und Anlage), Speicherfristen (§ 100a Abs. 4 Kernbereich), Erforderlichkeitsgrundsatz, Datenvermeidung und Datensparsamkeit (§ 7 Abs. 4 NDSG, § 100a StPO Verwertungsverbot), Transparenzregeln (Volkszählungsurteil BVerfG, § 100a Abs. 4 StPO Dokumentation/aktenkundig machen, Revisionsfähigkeit), Mandantentrennung (Föderalismus)

SDM
Standard-Datenschutzmodell

TK-Überwachungsobjekte

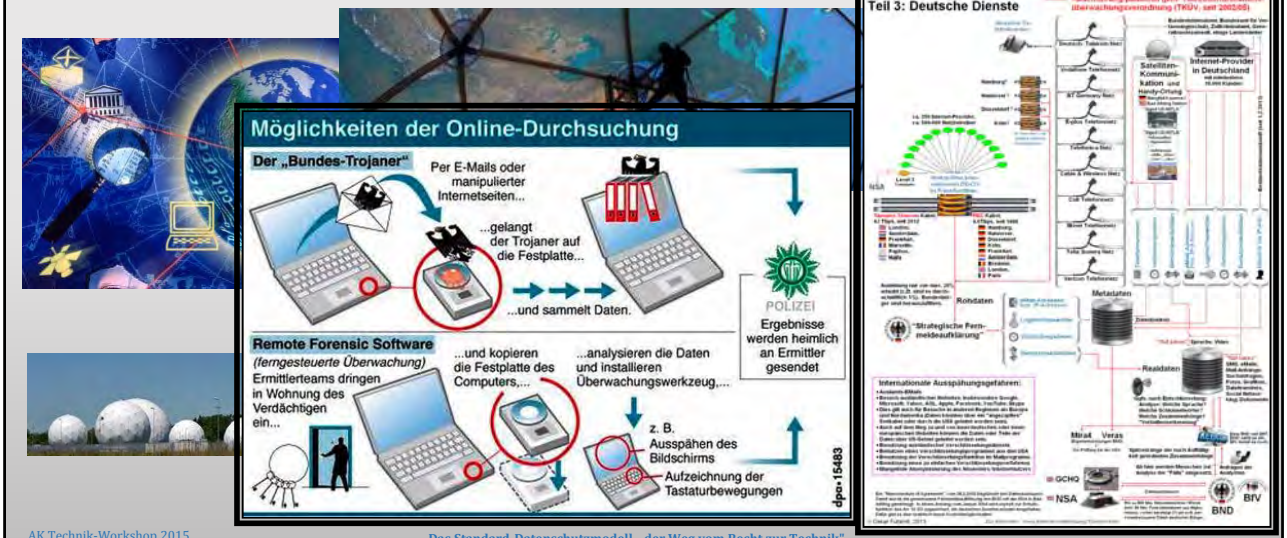
- Telefonie
- IP-Datenverkehr
- Video-Streaming
- Datentransfer
- VoIP-Telefonie



Bildnachweis: Wikimedia Common Lizenz

SDM
Standard-Datenschutzmodell

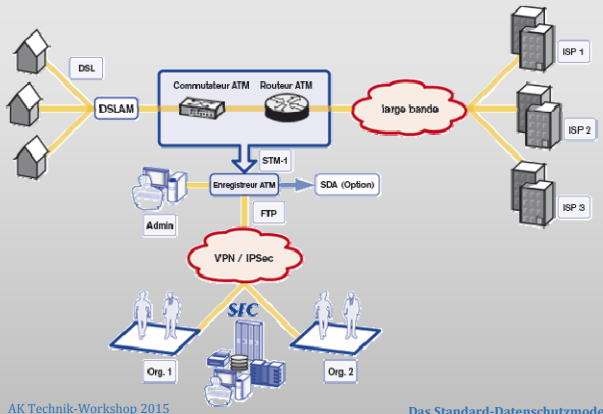
TKÜ-Varianten i.w.S.



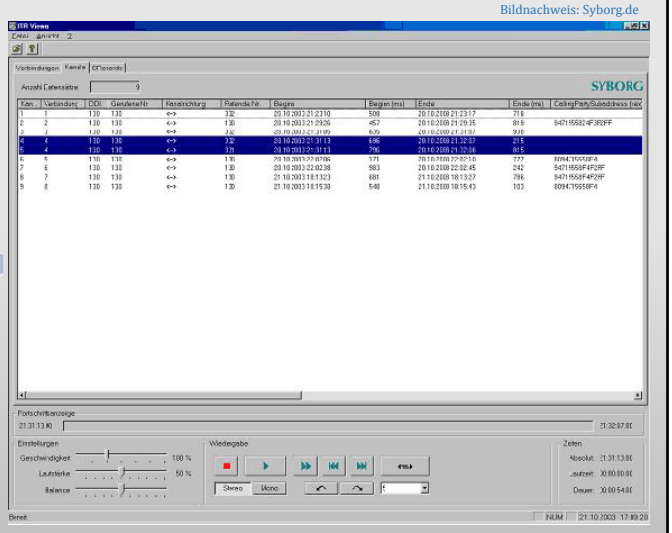
SDM
Standard-Datenschutzmodell

TKÜ-Verfahren

Prinzipskize und Recording-Tool
der Fa. SYBORG Informationssysteme



Bildnachweis: Syborg.de



Modellierung nach SDM

- Anforderungen: Minimierung von Überwachung und Daten! Ausschluss/Begrenzung von:
  - Erhebung (keine überbordenden Datenstreams, zeitlich und sachlich auf Anordnungsmaß begrenzt, Kernbereichsschutz umsetzen),
  - Nutzung der erhobenen TKÜ Daten (nur für den Anordnungsfall),
  - Zahl der Betroffenen (Unbeteiligtenschutz)

- Gewährleistungsziele, Schutzbedarf, Referenzmaßnahmen
- Betrachtung der Daten, Systeme, Prozesse

Analyse des Schutzbedarfs

	Daten	Systeme	Prozesse
Datensparsamkeit	Gesetzliche Vorgaben	Vererbt	Vererbt
Verfügbarkeit	hoch	Vererbt	Vererbt
Integrität	sehr hoch	Vererbt	Vererbt
Vertraulichkeit	Erhöhte Anforderungen wegen Missbrauchspotenzial und Schadenshöhe Leib und Leben	Vererbt	Vererbt
Nichtverkettbarkeit	Erhöhte Anforderungen wegen Missbrauchspotenzial	Vererbt	Vererbt
Intervenierbarkeit	Information der Betroffenen erst nach Durchführung	Normal	Normal
Transparenz	Gesetzliche Vorgaben	Vererbt	Vererbt

SDM
Standard-Datenschutzmodell

Überblick über die (generischen) Referenzmaßnahmen

	Daten	Systeme	Prozesse
Datensparsamkeit	Reduzierung von Daten, Verfälschung, Trennung, Begrenzung	Reduzierung von Verarbeitungen, Sperrung, Löschung, Pseudonymisierung/Annonymisierung	Gewaltenteilung, Kontrolle, Löschprozesse, Beschränkung Berechtigter
Verfügbarkeit	Schutz der Daten, Syntax und Semantik	Schutz der Systeme	Planung, Überwachung, Notfall
Integrität	Protokollierung, Rechte, Hashes	Rechte, Prüfungen	Planung, Rechte/Rollen
Vertraulichkeit	Rechte, Protokollierung, Verschlüsselung	Kontrolle, Verschlüsselung	Rechte/Rollen, Regelungen, Kontrolle
Nichtverkettbarkeit	Trennung, Anonymisierung, Löschung, Mandantentrennung	Trennung auf Systemebene, Mandantentrennung	Rechte/Rollen/Identitäten, Kontrolle, Mandantentrennung
Intervenierbarkeit	Schaffung notwendiger Datenfelder	Änderbarkeit und Steuerung	Änderbarkeit und Nachverfolgbarkeit
Transparenz	Dokumentation der Daten (Formate, Syntax, Erforderlichkeit)	Dokumentation der Systeme (physisch, logisch, über Zustände)	Dokumentation, Versionierung, Änderungsverfahren

SDM
Standard-Datenschutzmodell

Referenzmaßnahmen Integrität

Daten

- ID1: Einschränkung von Schreib- und Änderungsrechten
- ID2: Protokollierung von schreibenden/ändernden Zugriffen
- ID3: Protokollierung geänderter Daten
- ID4: Technische Integritätskontrollen (Signaturen/Hashes)
- ID5: Ausgabe von Quittungen

Systeme

- IT1: Einschränkung von schreibenden Zugriffen/Konfigurationsmöglichkeiten auf IT-Systemen (z. B. Netztrennung durch Sicherheitsgateways)
- IT2: Regelmäßige Integritätsprüfung/Audits
- T3: Einsatz von Trusted Computing

Prozesse Technik/Organisation

- IPo1:Detaillierte Planungen von Verfahren und Verfahrensschritten
- IPo2: Geordnete Zuweisung von Rechten und Rollen
- IPo3: Geordnete Änderung von Verfahren und Verfahrensschritten
- IPt1: Regelmäßige Überprüfung zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen
- IPt2: Prozesse zur Aufrechterhaltung der Aktualität von Daten
- IPt3: Festlegung des Sollverhaltens von Prozessen

SDM
Standard-Datenschutzmodell

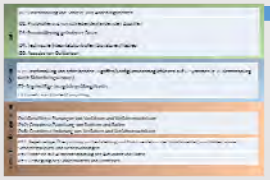
Konkrete Maßnahmen Integrität

Daten:

- Eine Einschränkung von Schreib- und Änderungsrechten auf Daten erfolgt durch das Setzen bzw. den Entzug entsprechender Rechte
- Das Schreiben/Ändern der Daten wird protokolliert
- Die geänderten Daten werden protokolliert (Versionen)
- Durch Signaturen/Hashes wird eine Veränderung von Daten überprüfbar
- Die Ausgabe von Quittungen dient der Bestätigung des Empfangs einer bestimmten Information oder eines Datenpaketes

SDM
Standard-Datenschutzmodell

Konkrete Maßnahmen Integrität



Systeme:

- Eine Einschränkung von Zugriffen/ Konfigurationsmöglichkeiten erfolgt auf Systemebene durch das Setzen bzw. den Entzug entsprechender Rechte.
- Durch eine regelmäßige Prüfung wird die Wirksamkeit getroffener Maßnahmen überprüft.
- Es wird die Integrität sowohl der Software-Datenstrukturen als auch der Hardware überwacht

SDM
Standard-Datenschutzmodell

Konkrete Maßnahmen Integrität

Technik/Organisation

Prozesse:

- Durch detaillierte Planungen von Verfahren und Verfahrensschritten wird die Funktion von Prozessen ermöglich
- Durch die Zuweisung von Rechten und Rollen wird der korrekte Ablauf der Prozesse ermöglicht
- Durch die geordnete Änderung von Verfahren und Verfahrensschritten wird der korrekte Ablauf von Prozessen ermöglicht
- Durch regelmäßige Überprüfung von Verfahren soll die Wirksamkeit getroffener Regelungen evaluiert werden
- Durch geregelte Prozesse und Vorgehensweisen bei der Überprüfung der Aktualität der Daten
- Festlegung der Überwachung von Fehlverhalten in Prozessen

AK Technik-Workshop 2015
Hannover, 29.04.2015

„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen

13

SDM
Standard-Datenschutzmodell

Das Team SDM bedankt sich für Ihre Aufmerksamkeit!

AK Technik-Workshop 2015
Hannover, 29.04.2015

„Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik"
Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen

14

Usecase aus dem Privatbereich: GPS-Überwachung von Firmenfahrzeugen

Lars Konzelmann
Referent beim Sächsischen Datenschutzbeauftragten

Inhalt

- Ausgangslage/erste juristische Bewertung
- Möglichkeiten von GPS-Tracking
- Modellierung nach SDM
- Schutzbedarfsanalyse
- Überblick über die Referenzmaßnahmen
- Bespiel: Maßnahmen der Vetraulichkeit

Ausgangslage/erste juristische Bewertung

- Firma setzt GPS-Überwachung von Firmen-Fuhrpark ein
- Zweck: Diebstahlschutz, Disposition von Aufträgen (bundesweit), Mitarbeiterüberwachung (???)
- Juristische Prüfung:
  potentiell zur Verhaltens- und Leistungskontrolle geeignet
- Rechtsgrundlage: Disposition: § 32 Abs. 1 BDSG
  Einschränkung: „Live"-Beobachtung, keine Speicherung
- Zu beachten: TOM (§ 9 BDSG), Datenvermeidung und Datensparsamkeit (§ 3a BDSG), Transparenzregeln (§§ 4 Abs. 3, 6c Abs. 1 BDSG)

Möglichkeiten von GPS-Tracking

Quelle: http://www.bornemann.net

Modellierung nach SDM

- Anforderungen: Keine Speicherung! Ausschluss/Begrenzung von Missbrauch

  > Technik muss erst datenschutzkonform gemacht werden!

- Gewährleistungsziele, Schutzbedarf, Referenzmaßnahmen
- Betrachtung der Daten, Systeme, Prozesse

Analyse des Schutzbedarfs

	Daten	Systeme	Prozesse
Datensparsamkeit	Erhöhte Anforderungen wegen Missbrauchspotenzial und allg. jur. Vorgaben	Vererbt	Vererbt
Verfügbarkeit	Normal	Normal	Normal
Integrität	Normal	Normal	Normal
Vertraulichkeit	Erhöhte Anforderungen wegen Missbrauchspotenzial	Vererbt	Vererbt
Nichtverkettbarkeit	Erhöhte Anforderungen wegen Missbrauchspotenzial	Vererbt	Vererbt
Intervenierbarkeit	Normal	Normal	Normal
Transparenz	Erhöhte Anforderungen wegen Missbrauchspotenzial	Vererbt	Vererbt

SDM
Standard-Datenschutzmodell

Überblick über die Referenzmaßnahmen

	Daten	Systeme	Prozesse
Datensparsamkeit	Reduzierung von Daten, Verfälschung, Trennung, Begrenzung	Reduzierung von Verarbeitungen, Sperrung, Löschung, Pseudo./Annon.	Gewaltenteilung, Kontrolle, Löschprozesse
Verfügbarkeit	Schutz der Daten, Syntax und Semantik	Schutz der Systeme	Planung, Überwachung, Notfall
Integrität	Protokollierung, Rechte, Hashes	Rechte, Prüfungen	Planung, Rechte/Rollen
Vertraulichkeit	Rechte, Protokollierung, Verschlüsselung	Kontrolle, Verschlüsselung	Rechte/Rollen, Regelungen, Kontrolle
Nichtverkettbarkeit	Trennung, Anonymisierung, Löschung	Trennung auf Systemebene	Rechte/Rollen/Idenditäten, Kontrolle
Intervenierbarkeit	Schaffung notwendiger Datenfelder (Betroffenenrechte)	Änderbarkeit und Steuerung (zur Wahrung der Betroffenenrechte)	Änderbarkeit und Nachverfolgbarkeit
Transparenz	Dokumentation der Daten (Formate, Syntax, Erforderlichkeit)	Dokumentation der Systeme (physisch, logisch, über Zustände)	Dokumentation, Versionierung, Änderungsverfahren

SDM
Standard-Datenschutzmodell

Referenzmaßnahmen Vertraulichkeit

Daten	CD1: Einschränkung von Leserechten (für Datenverarbeiter, ggf. durch den Nutzer selbst)
	CD2: Protokollierung lesender Zugriffe
	CD3: Verschlüsselung der Daten
Systeme	CT1: Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle
	CT2: Verschlüsselung auf System- und Transportebene
	CT3: Spezifizierte, für das Verfahren ausgestattete Umgebungen (Gebäude, Räume)
Prozesse Technik/Organisation	CPt1: Festlegung eines Rechte-Rollen-Konzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentisierungsverfahrens
	CPt2: Kryptokonzept
	CPo1: Verpflichtung auf das Datengeheimnis (BDSG)
	CPo2: Verschwiegenheitsvereinbarungen
	CPo3: Eingrenzung der zulässigen Personalkräfte (zuständig, befähigt, zuverlässig (ggf. sicherheitsüberprüft), keine Interessenskonflikte)
	CPo4: Schutz vor äußeren Einflüssen (Spionage)
	CPo5: Geregelte Außerbetriebnahme von Geräten und Sicherstellung der Entsorgung von Datenträgern
	CPo6: Umgang mit Mitarbeiterdaten in den Bereichen Personal und betriebliche Überwachung (Videokontrolle, Protokollierung von Zugängen und Nutzung von Technik)
	CPo7: Regelungen zum mobilen Arbeiten und zu externen Zugängen
	CPo8: Regelungen zum Versand /Transport von Datenträgern

SDM
Standard-Datenschutzmodell

Konkrete Maßnahmen Vertraulichkeit

Daten:

- Protokollierung der lesenden Zugriffe unter Benennung des Grundes
- Verschlüsselung der Daten auf Transportebene, ggf. am Speicherort
- Zugriffe des ADV ggf. Unterauftragnehmer (Bsp. Kartendienstleister)

SDM
Standard-Datenschutzmodell

Konkrete Maßnahmen Vertraulichkeit

Systeme:

- Dokumentiertes System (Handbücher, Administrationsvorgaben)
- Eingesetzte Verschlüsselungstechnologien
- Unterbringung der Systeme ggf. beim ADV

SDM
Standard-Datenschutzmodell

Konkrete Maßnahmen Vertraulichkeit

Prozesse:

- Rechte- und Rollenkonzept
- Vertragliche Regelungen
- Zugriffsberechtigtes Personal
- Prozesse bei der Disposition und im Diebstahlsfall

SDM
Standard-Datenschutzmodell

Das Team SDM
bedankt sich für
Ihre Aufmerksamkeit und
wünscht allen
eine gute Heimreise!

Das Standard-Datenschutzmodell

Konzept zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele

V.0.8a nach Vorlage in der 66. Sitzung des AK Technik am 10. und 11. September 2014 in Schwerin und in der 89. Sitzung der DSK am 18. und 19. März 2015 in Wiesbaden in der Sitzung der UAG SDM am 20. und 21. April 2015 redaktionell überarbeitet

Inhalt

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, Datensicherheit und Nachvollziehbarkeit der Prüftätigkeit 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 für ein Verfahren kann konkrete Maßnahmen vorschreiben, so z. B. eine Anonymisierung erhobener personenbezogener Daten, sobald ein bestimmter Zweck der Verarbeitung erreicht wurde. Andererseits können ggf. weitere, besondere Maßnahmen ergriffen werden, die nicht explizit gesetzlich vorgeschrieben sind, um bei einer rechtlich gebotenen Interessensabwägung zusätzlich berücksichtigt zu werden.

In beiden Fällen stehen neben den verfahrensspezifisch ergriffene 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, was einer engen Bestimmung im Sinne der IT-Sicherheit entspräche. 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 übergreifende Gewährleistungsziel Datensparsamkeit

Das Gewährleistungsziel *Datensparsamkeit* wird hier als übergreifendes Gewährleistungsziel betrachtet, weil es über den technischen Aspekt der Datenverarbeitung hinaus den vollständigen Lebenszyklus personenbezogener Daten von der Erhebung über die Verarbeitung und Nutzung bis zur Löschung personenbezogener Daten umfasst. Damit betrifft dieses Gewährleistungsziel – anders als die in Abschnitt 5.4 beschriebenen elementaren Gewährleistungsziele – nicht nur den Umgang mit bereits vorhandenen personenbezogenen Daten, sondern ist als Gestaltungsanforderung informationstechnischer Systeme von grundlegender Bedeutung. Das Gewährleistungsziel Datensparsamkeit verpflichtet somit verantwortliche Stellen zum umfassenden Systemdatenschutz und wirkt sich dadurch auf die Gewährleistung aller anderen elementaren Gewährleistungsziele aus. Die Grafik in Abschnitt 10.3 verdeutlicht dies, indem das Gewährleistungsziel Datensparsamkeit über den sechs elementaren Gewährleistungszielen steht. Die Regelung adressiert nicht nur die verantwortliche Stelle sondern indirekt auch Hersteller und Anbieter von informationstechnischen Systemen, da diese die Gestaltungsanforderungen bei der Entwicklung der Technik umzusetzen haben.

Datensparsamkeit konkretisiert den Grundsatz der Erforderlichkeit, der vom Verarbeitungsprozess 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 sowohl bei der Gestaltung des Erhebungsvorgangs als auch bei den Kernprozessen des Verfahrens und bei ihrer Ausführung und Unterstützung zum Beispiel im Kontext der Wartung der verwendeten Systeme zu berücksichtigen.

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 wird. Ausgehend von

Zwecksetzung und Datengrundlage können Abfolgen von Verarbeitungsschritten danach bewertet werden, ob in ihrem Rahmen die Verfügungsgewalt über die zu erhebenden Daten und die Verbreitung von Kenntnissen über die Betroffenen ausreichend minimiert wird. Im Ergebnis kann im Einzelnen die Erforderlichkeit von beispielsweise Datenfeldern, Schnittstellen oder Hilfsprozessen beurteilt werden.

Der Grundsatz der Datensparsamkeit geht davon aus, dass der beste Datenschutz darin besteht, keine oder möglichst wenige personenbezogene Daten verarbeiten zu müssen. Zielvorgabe des Gewährleistungsziels Datensparsamkeit ist eine Optimierung mit dem Ziel, die jeweils datensparsamste Art der Datenverarbeitung zu wählen. Das Optimierungsziel ist mit dem o. g. Bewertungskriterium der Minimierung von Verfügungsgewalt und Kenntnisnahme 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.

Das Ziel der Datensparsamkeit kann durch frühestmögliche Löschung nicht weiter benötigter personenbezogener Daten, aber auch durch Abstufungen auf der Ebene der verschiedenen Verarbeitungsschritte erreicht werden. Dies kann insbesondere durch Reduktion der Datenmenge , durch Minimierung des Personenbezugs (Anonymisierung, Pseudonymisierung) der zu verarbeitenden oder zur Kenntnis gegebenen Daten als auch durch technische Einschränkung der Verarbeitungsmöglichkeiten erreicht werden.

Datenvermeidung als Sonderfall der Datensparsamkeit

Das Bundesdatenschutzgesetz benutzt als Überschrift für § 3a das Begriffspaar „Datenvermeidung und Datensparsamkeit“. In diesem Dokument wird ausschließlich der Begriff Datensparsamkeit verwendet, da Datenvermeidung lediglich der stets anzustrebende Sonderfall der Datensparsamkeit ist. Mit der Datenvermeidung ist das Optimum erreicht, da in diesem Fall personenbezogene Daten gar nicht erst erhoben werden.

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 organisations-externen 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 Duplizierung 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 Übernahme eines Datenbestandes Bezeichnung und Revisionsstand des Quelldatenbestandes sowie ein Verweis auf dessen Dokumentation.

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

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

6 Der Bezug der Gewährleistungsziele zum bestehenden Datenschutzrecht

6.1 Gewährleistungsziele in der Rechtsprechung des Bundesverfassungsgerichts

Die Gewährleistungsziele Transparenz und Intervenierbarkeit spielen im Volkszählungsurteil von 1983, in dem das Recht auf informationelle Selbstbestimmung begründet wurde, eine maßgebliche Rolle.

Das Bundesverfassungsgericht hat im Februar 2008 Gewährleistungsziele unmittelbar aus den Verfassungsnormen abgeleitet, indem es das Grundrecht „auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ formulierte (BVerfG, 1 BvR370/07 vom 27.02.2008).

6.2 Verankerung der Gewährleistungsziele im BDSG

6.2.1 Gewährleistungsziele als Prüfungsmaßstab

Ausgangspunkt ist § 9 BDSG:

> *„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.“*

Die Gewährleistungsziele müssen also, sofern Sie nicht bereits durch die in der Anlage zu diesem Gesetz genannten Anforderungen abgedeckt werden, sich aus den übrigen „Vorschriften dieses Gesetzes“ ergeben. Anderenfalls kann ein Verstoß gegen die Gewährleistungsziele nicht sanktioniert werden bzw. können keine Maßnahmen nach § 38 Abs. 5 Satz 1 BDSG zur Beseitigung technischer oder organisatorischer Mängel angeordnet werden.

Zu beachten ist dabei, dass die Entscheidung des Gesetzgebers, in der Anlage zu § 9 bestimmte Anforderungen festzuschreiben, nicht durch Gewährleistungsziele ersetzt werden können. Die gesetzlichen Anforderungen sind „insbesondere“ zu prüfen.

Auch wenn die Anforderungen aus einem Kontext zentral organisierter Rechenzentren stammen, der nicht mehr die heutige Realität darstellt, so können die Gewährleistungsziele diese nur dann ersetzen, wenn man den Gesetzestext entsprechend auslegt. In Betracht kommen dafür die „grammatische Auslegung“, die „systematische Auslegung“, die „historische Auslegung“ und die „teleologische Auslegung“.

Aber weder der Wortlaut, der Zusammenhang, die Entstehungsgeschichte oder der Sinn und Zweck des § 9 BDSG ermöglichen eine Ersetzung der ausdrücklich festgeschriebenen Maßnahmen durch Gewährleistungsziele. Vielmehr ist der Bundesgesetzgeber, anders als die Landesgesetzgeber, der Anregung des AK Technik (7. TB SächsDSB/14.6), die „10 Gebote“ durch technikunabhängige Gewährleistungsziele zu ersetzen, nicht gefolgt. Es wurde

durch den AK Technik bereits damals (nur) gefordert, § 9 BDSG bzw. die entsprechenden Ländervorschriften zu ändern – eine Anwendung ohne eine Gesetzesänderung wurde zu Recht nicht erwähnt.

Vorrangig hat eine Prüfung der technisch-organisatorischen Maßnahmen daher nach der Anlage zu § 9 BDSG zu erfolgen. Im Folgenden wird daher dargestellt, inwieweit die Gewährleistungsziele bereits durch die Anlage zu § 9 BDSG abgedeckt sind bzw. sich aus materiellrechtlichen Grundlagen herleiten lassen.

Auf die entsprechenden Bestimmungen der Datenschutzrichtlinie (DSRL) wird hingewiesen, da es sich bei dieser nach der Entscheidung des EuGH (C-468/10 und C-469/10) vom 24.11.2011 um eine Vollharmonisierung handelt. Das bedeutet, dass die Anforderungen grundsätzlich weder über- noch unterschritten werden dürfen.

6.2.2 Verankerung der Gewährleistungsziele im BDSG

Die nachfolgenden Erörterungen zur gesetzlichen Verankerung der Gewährleistungsziele beziehen sich zunächst nur auf die Datenebene. Im Hinblick auf die gesetzliche Verankerung der Anwendbarkeit der Gewährleistungsziele auf personenbezogene Verfahren werden in Abschnitt 6.3.3 nähere Ausführungen gemacht.

Zu berücksichtigen ist, dass die Gewährleistungsziel-Anforderungen nur auf die jeweils materiellrechtlich ableitbaren Anforderungen begrenzt sind. So wird man beispielsweise keine allumfassende Transparenz fordern können.

Datensparsamkeit

Die Datensparsamkeit ist in § 3a BDSG geregelt. Darüber hinaus ergibt sie sich aus dem allgemeinen Grundsatz der Erforderlichkeit, der in den einzelnen Verarbeitungsschritten erwähnt wird oder der Anonymisierungspflicht in § 30 a Abs. 3.

Zu beachten ist in diesem Zusammenhang aber auch die Löschpflicht bei weggefallener Erforderlichkeit (§ 20 Abs. 2 Nr. 2 und § 35) oder dem Ablauf von spezialgesetzlichen Aufbewahrungsfristen.

Verfügbarkeit

Dieses Gewährleistungsziel ist bereits in der Nr. 7 der Anlage zu § 9 BDSG als zu treffende Maßnahme aufgeführt. Art. 17 Abs. 1 Satz 1 DSRL fordert geeignete Maßnahmen für einen Schutz gegen die zufällige oder unrechtmäßige Zerstörung oder den zufälligen Verlust personenbezogener Daten. Eine zeitgerechte Zugriffsmöglichkeit ist nicht erwähnt.

Eine explizite entsprechende materiellrechtliche Verpflichtung ist weder dem BDSG noch der DSRL zu entnehmen.

Integrität

Maßnahmen nach Nr. 1-6 der Anlage zu § 9 BDSG dienen der Erreichung von Integrität. Art. 17 Abs. 1 DSRL 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“.

Materiellrechtlich gibt es in § 20 bzw. § 35 Abs. 1 BDSG eine Pflicht zur Berichtigung und der entsprechenden Benachrichtigung – ebenso in Art. 12 DSRL.

Vertraulichkeit

Maßnahmen nach Nr. 1-6 der Anlage zu § 9 BDSG dienen auch der Erreichung von Vertraulichkeit. Art. 17 Abs. 1 DSRL fordert geeignete Maßnahmen für einen Schutz gegen eine unberechtigte Weitergabe oder den unberechtigten Zugang.

Materiellrechtlich gibt es in § 5 BDSG bzw. Art. 16 DSRL Regelungen zum „Datengeheimnis“ bzw. zur „Vertraulichkeit“.

Nichtverkettbarkeit

Die Nichtverkettbarkeit kann durch Maßnahmen nach Nr. 8 der Anlage zu § 9 BDSG erreicht werden. Eine entsprechende Vorschrift ist in der DSRL nicht zu finden.

Materiellrechtlich ergibt sich die Verpflichtung zur Festlegung der Zwecke insbesondere 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 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 die Erforderlichkeit der Datenverarbeitung ist den einzelnen Verarbeitungsbefugnissen zu entnehmen.

Die DSRL fordert in Art. 6 b) lediglich, dass eine Weiterverarbeitung **vereinbar** mit dem ursprünglichen Zweck sein muss.

Transparenz

Für die Betroffenen sind sowohl in der RL 95/46/EG (Art. 10, 11, 12) als auch im BDSG (§§ 4 Abs. 3, 4a Abs. 1 Satz 2, 33, 34) Informations-, Benachrichtigungs- und Auskunftsrechte geregelt.

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 kann.

Intervenierbarkeit

Verfahren sollen so gestaltet werden, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung wirksam ermöglichen. Dies ist durch die entsprechenden Regelungen im BDSG abgedeckt. Soweit darüber hinaus jedoch gefordert wird, dass dies „jederzeit“ möglich sein soll, ist dies nicht abgedeckt.

Tabelle: Zuordnung der gesetzlichen Vorgaben zu den Gewährleistungszielen.

Datensparsamkeit	**Verfügbarkeit**	**Integrität**	**Vertraulichkeit**	**Nichtverkettbarkeit**	**Transparenz**	**Intervenierbarkeit**
	Nr. 7 der Anlage zu § 9	Nr. 1-6 der Anlage zu § 9	Nr. 1-6 sowie Satz 2 der Anlage zu § 9	Nr.8 der Anlage zu § 9		
§ 3a				§ 4 Abs. 3 Nr. 2	§ 4 Abs. 3	§ 4 Abs. 1
§ 4 Abs. 2 Nr. 2a				§ 4a Abs. 1 Satz 2	§ 4a Abs. 1 Satz 2-4, Abs. 2 Satz 2, Abs. 3	§ 4c Abs. 1 Satz 1 Nr. 1
§ 6 b Abs. 3, 5				§ 4b Abs. 6	§ 4d Abs. 1 Satz 1, § 4d Abs. 5	§ 6 Abs. 1, § 6 Abs. 2 Satz 1
§ 13 Abs. 1, Abs. 2 Nr. 3, 5, 6, 7, 8, 9				§ 4c Abs. 1 Satz 2	§ 4e	§ 6a Abs. 2 Nr. 2
				§ 4e Nr. 4		

§ 14 Abs. 1, Abs. 2 Nr. 6, 7, 8, 9, Abs. 5 Nr. 2				§ 6b Abs. 1, Abs. 3, Abs. 5	§ 4g Abs. 2	§§ 19-21
§ 15 Abs. 1 Nr. 1				§ 10 Abs. 2 Nr. 1	§ 6 Abs. 2 Satz 3	§§ 33-35
§ 16 Abs. 1 Nr. 1				§ 11 Abs. 2 Nr. 2	§ 6a Abs. 2 Nr. 2, § 6a Abs. 3	
§ 20 Abs. 2 Nr. 2, Abs. 6				§ 14	§ 6b Abs. 2, Abs. 4	
§ 28 Abs. 1 Nr. 1, Nr. 2, Abs. 2 Nr. 2 und 3, Abs. 3, Abs. 6 Nr. 1, 3, 4, Abs. 8, 9				§ 15 Abs. 3	§ 6c Abs. 1, Abs. 3	
§ 28 a Abs. 1				§ 16 Abs. 4	§ 10 Abs. 3	
§ 30 Abs. 1				§ 28 Abs. 1 Satz 2, Abs. 5, Abs. 8	§§ 19, 19a	
§ 30 a Abs. 3				§ 31	§ 28 Abs. 4, § 28a Abs. 2,3, § 29 Abs. 7	
§ 35 Abs. 2				§ 39	§§ 33, 34, 38	

6.2.3 Verankerung der Anwendbarkeit der Gewährleistungsziele auf personenbezogene Verfahren

Unproblematisch ist, dass die materiellrechtlichen Vorgaben zumeist an konkrete Datenverarbeitungen anknüpfen, die Gewährleistungsziele aber unabhängig davon bereits bei der Verfahrensgestaltung berücksichtigt werden 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). Ausdrücklich wird auf Verfahren im Rahmen der Meldepflichten und Vorabkontrollen abgestellt (§ 4e); bei letzteren findet naturgemäß noch keine Verarbeitung personenbezogener Daten statt.

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

Dem steht auch die Entscheidung des Bundesverfassungsgerichts zum „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ nicht entgegen. Darin hat es – zu einem Zeitpunkt, in dem die o.g. Vorschriften bereits geraume Zeit in Kraft waren – festgestellt, dass „informationstechnische Systeme“ auch dann geschützt sind, wenn auf ein solches System zugegriffen wird, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein (BVerfG, 1 BvR 370/07, Rn. 200). Soweit ein Personenbezug besteht, sind sie jedoch vom Grundrecht auf informationelle Selbstbestimmung umfasst und müssen sich an den Anforderungen für die Verarbeitung personenbezogener Daten messen lassen. Im Übrigen dürften gesetzliche Vorgaben für die Gestaltung von Verfahren zur Verarbeitung personenbezogener Daten keinen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme darstellen, weil Anforderungen an und Vorgaben für das Verfahren nicht mit einem Zugriff auf dieses Verfahren gleichzusetzen sind.

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: Zuordnung der gesetzlichen Vorgaben zu den Gewährleistungszielen nach SächsDSG.

Datensparsamkeit	**Verfügbarkeit**	**Integrität**	**Vertraulichkeit**	**Nichtverkettbarkeit**	**Transparenz**	**Intervenierbarkeit**
§ 9 Abs. 1 Satz 2	§ 9 Abs. 2 Nr. 3	§ 9 Abs. 2 Nr. 2	§ 9 Abs. 2 Nr. 1		§ 9 Abs. 2 Nrn. 4-6	
§§ 20, 21 Abs. 2 Satz 2 (Löschung /Sperrung bei entfallener Erforderlichkeit)				§ 4 Abs. 3 (Zweckfestlegung bei Einwilligung)	§ 4 Abs. 3 (informierte Einwilligung)	§ 4 Abs. 1 Nr. 2 (Einwilligung/Rücknahme)
§ 36 Abs. 2 (Pseudonymisierung/Anonymisierung bei wiss. Forschung)				§ 10 Abs. 1 Nr. 2 (Zweckbestimmung im Verfahrensverzeichnis)	§ 5 (Betroffenenrechte)	§§ 19-21 (Berichtigung, Löschung, Sperrung)
§ 33 Abs. 4 (Löschfrist bei Videoaufzeichnungen)				§ 12 Abs. 2, 5, 6 (Zweckfestleung bei Erhebung)	§3 10, 11 Abs. 4 Nr. 5, 31 Abs. 2 (Verfahrensverzeichnis)	§ 32 Abs. 1 (Fernmessen und Fernwirken)
§ 12 (Erhebung nur bei Erforderlichkeit)				§ 13 (Zweckbindung bei Speicherung etc.)	§ 12 (Datenerhebung)	
§ 13 (Speicherung etc.				§§ 14 Abs. 3, 16 Abs. 4 (Zweckbindung bei	§§ 18, 34 Abs. 3 (Auskunft)	

nur bei Erforderlichkeit)				Übermittlung)		
§§ 14, 15, 16, 17 (Übermittlung nur bei Erorderlichkeit)				§ 32 Abs. 1 (Zweckbindung bei Fernmessen und Fernwirken)	§ 27 (Kontrolle)	
				§ 33 (Zweckbindung Video)	§ 32 (Fernmessen und Fernwirken)	
				§ 34 (automatisierte Einzelentscheidung)	§ 33 Abs. 3 (Videoüberwachnung)	

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 Infrastuktur,
- 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 folgende Eigenschaften und eigens zu betrachtende Schwerpunkte eine 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 eine (Teil-)Verantwortlichkeit zu klären, die typischerweise als Rolle in einem umfassenden Rollenkonzept formuliert und zugewiesen ist. 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. Dieser 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 Betroffenen	Eine Ansehens- oder Reputationsbeeinträchtigung ist zu erwarten, 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.

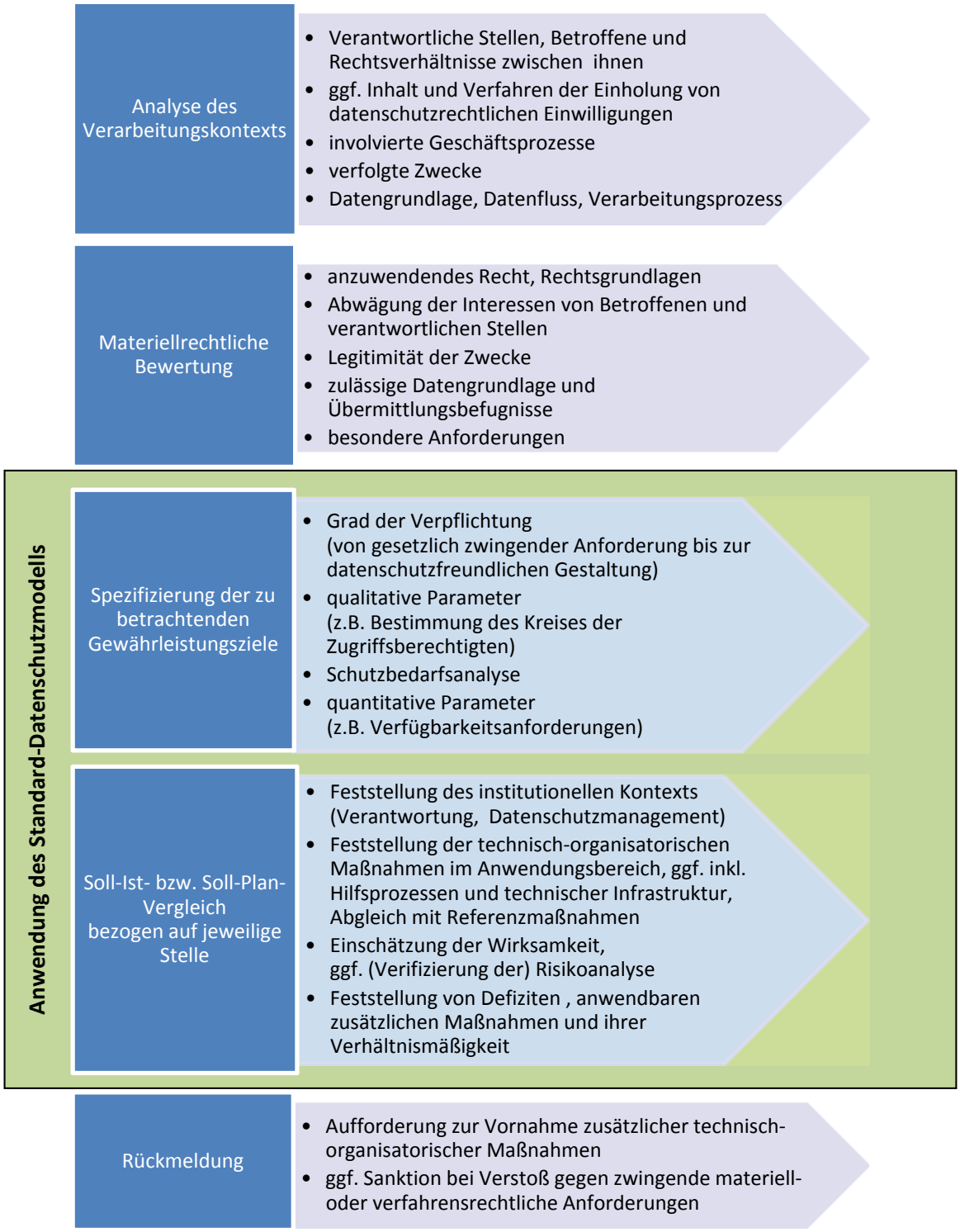


Abbildung 10.1: Die Anwendung des Standard-Datenschutzmodells im Rahmen von Prüf- und Beratungsvorgängen

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 10.1 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, welche Gewährleistungsziele betrachtet werden sollen, in welcher Ausprägung sie anzuwenden 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: 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:

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

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

10.2 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.

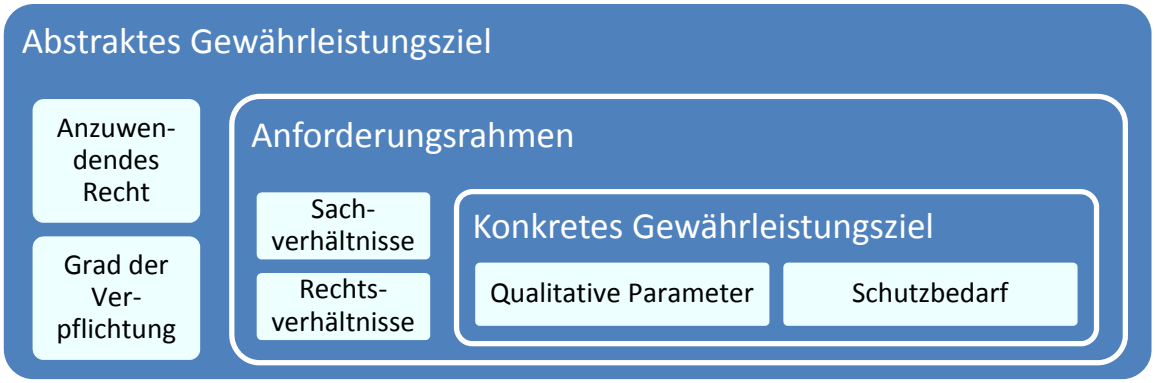


Abbildung 10.2: Spezifizierung der Gewährleistungsziele

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 materiellrechtlichen 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.

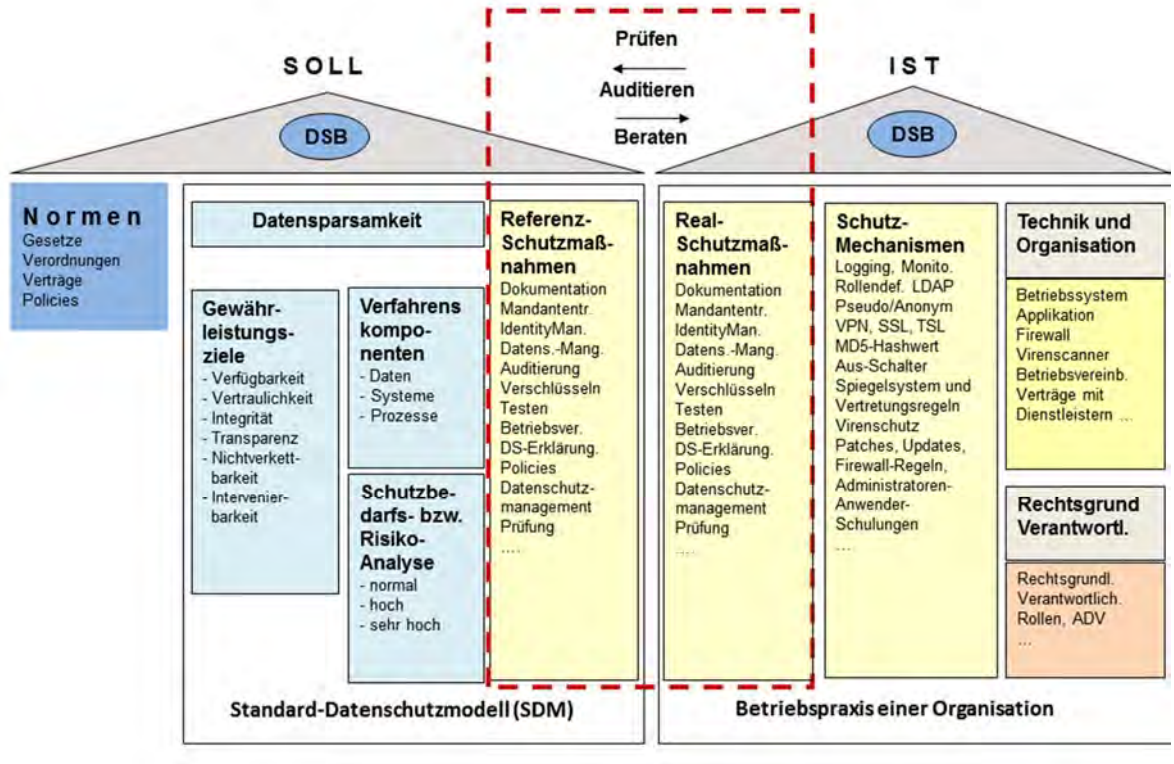


Abbildung 10.3: Der Soll-Ist-Vergleich

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 Anhang A: Katalog mit Standard-Datenschutzmaßnahmen

Tagungsband „Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik

Workshop 2015 des AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder