Eine kurze Geschichte des Prüfens

Martin Rost

13. Sicherheitskongress
des BSI, Bonn 2013-0514

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Datenschutz

Datenschutz…

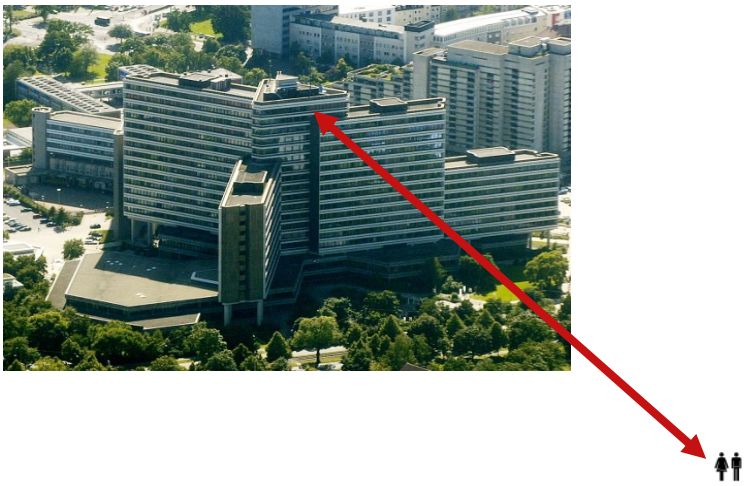
ist nicht nur das, was als Anforderungen im Datenschutzrecht steht (*juristischer Kurzschluss*).

ist nicht mit den Maßnahmen der Informationssicherheit gleichsetzbar (*technizistischer Kurzschluss*).

Was meint dann Datenschutz?

Objektbereich des Datenschutzes

Datenschutz beobachtet die organisierte Informationsverarbeitung und Kommunikation in der *asymmetrischen Machtbeziehung* zwischen Organisationen und Personen.



Objektbereich des Datenschutzes: Autonomieversprechen

Konkret sind das die *externen* Machtbeziehungen zwischen…

- öffentlicher Verwaltung und deren externen **Bürgern,**
- privaten Unternehmen und deren **Kunden,**
- IT-Infrastruktur-Providern und deren **Nutzern / Kunden** (bspw. Access-, Suchmaschinen-, Mail-, Socialnetwork-Betreiber);
- Praxen / Instituten / Gemeinschaften und deren **Patienten, Mandanten, Klienten;**
- Wissenschaftsorganisationen und deren Forschungsobjekten **Individuen, Subjekte, Menschen;**

sowie die *internen* Machtbeziehungen zwischen

- Organisationen (Arbeitgeber, auch: Kirche, Militär, (Sport-) Verein) und deren **Mitarbeitern der Mitgliedern** (Schüler, Patienten, Gefangenen, Soldaten, …).

Rost, Martin: **Zur Soziologie des Datenschutzes**, in: DuD 2013/02: 85-91.

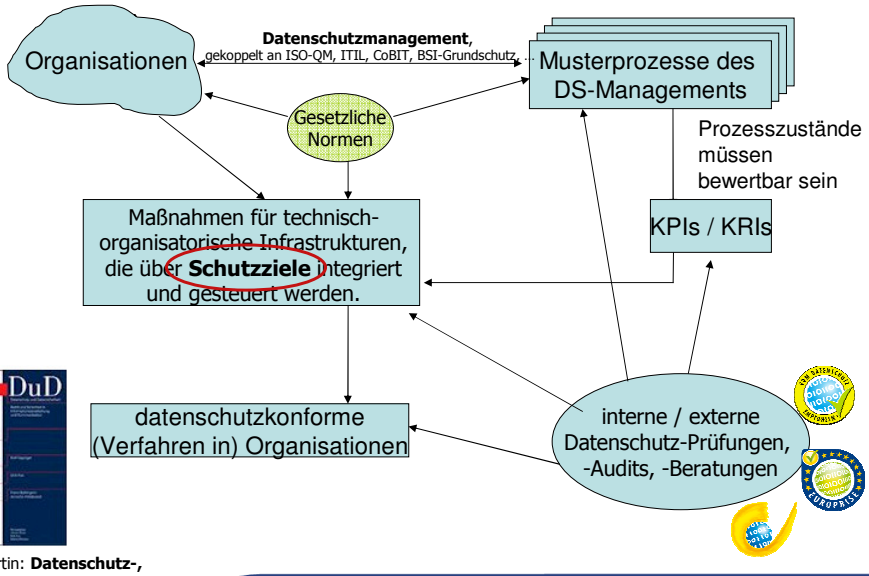
Zum Verhältnis von Datenschutz und Datensicherheit

- **Datensicherheit:**
  Die Person ist der Angreifer!
  Folge? Die Person muss nachweisen, dass sie kein Angreifer ist und dass sie ggfs. mit einem Zugriff auf ihre Person rechnen muss.
  Klassischer Schutz: Login/Authentisierung, Autorisierung der Person gegenüber Organisation, Rollenkonzepte, Kontrolle der MA.

- **Datenschutz:**
  Die Organisation ist der Angreifer!
  Folge? Die Organisation muss (jederzeit) prüffähig nachweisen (können), dass sie kein Angreifer ist, sich an die Regeln hält und bei all dem ihre Verfahren und Prozesse beherrscht.

- Gleichwohl gilt: Datenschutz kommt ohne Datensicherheit nicht aus.

Big Picture Prozesse, DS-Management, Schutzziele, KPI/KRI



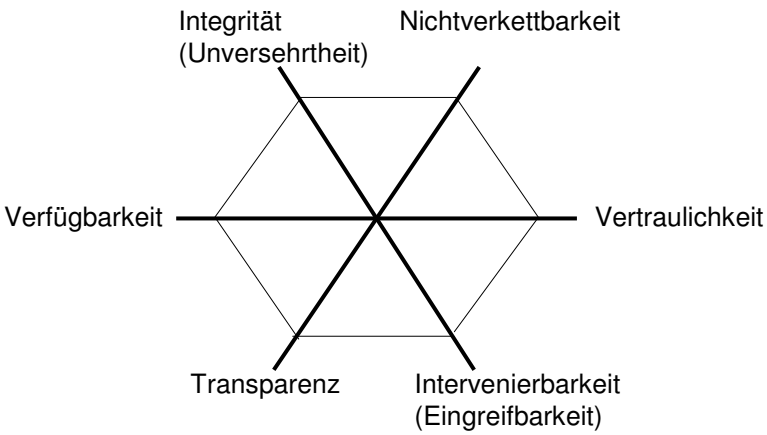
Rost, Martin: **Datenschutz-, Managementsystem**; in: DuD 2013/05: 295-300.

Zur Standardisierung von Datenschutz im Bereich technisch-organisatorischer Maßnahmen (SDM)

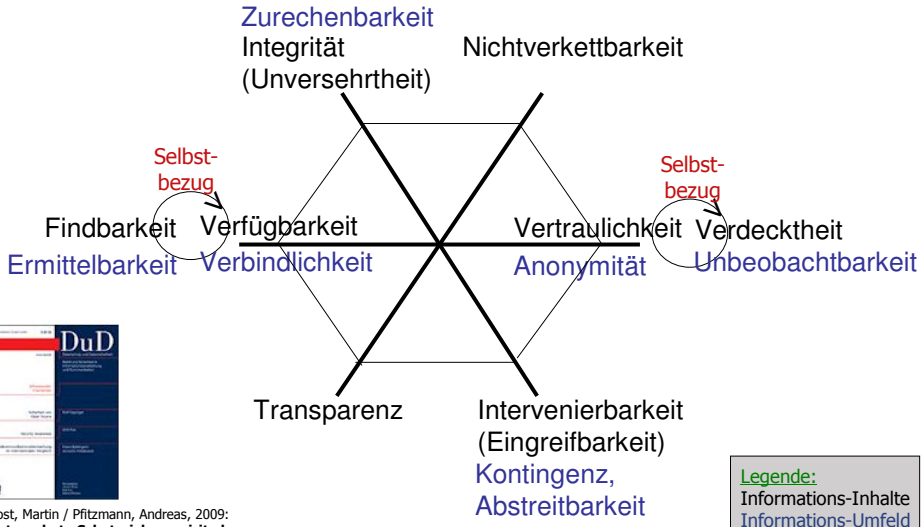
Ziel: Die **bewährte Methodik von Grundschutz** nutzen. Dabei jedoch die Unterschiede zwischen IT-Sicherheit und Datenschutz markieren. Das heißt:

1. Ergänzung der Risikodimensionen um **datenschutzeigene Schutzziele,** die durch **datenschutzeigene Schutzmaßnahmen** erfüllbar sind.
2. Definition der **Schutzbedarfe** aus der Betroffenensicht.
3. **Personenbezug auf Verfahren ausdehnen**, nicht bei Daten stehen bleiben.

Schutzziele Systematik



Schutzziele
Systematik, vollständig



Rost, Martin / Pfitzmann, Andreas, 2009:
Datenschutz-Schutzziele - revisited;
in: DuD - Datenschutz und Datensicherheit,
33. Jahrgang, Heft 6, Juli 2009: 353-358

Legende:
Informations-Inhalte
Informations-Umfeld

Schutzziele
in Gesetzen *(Bsp: NRW, textgleich: B und die 6 neuen Bundesländer,*

§ 10 Technische und organisatorische Maßnahmen (DSG-NRW)

(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen.

(2) Dabei sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass

- 1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können **(Vertraulichkeit)**,
- 2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben **(Integrität)**,
- 3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können **(Verfügbarkeit)**,
- 4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können **(Authentizität)**,
- 5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat **(Revisionsfähigkeit)**,
- 6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können **(Transparenz)**.

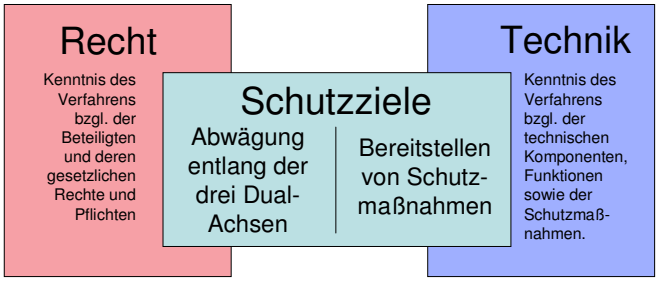
(3) (...)

Schutzziele im Gesetz (LDSG-SH, Januar 2012, §5)

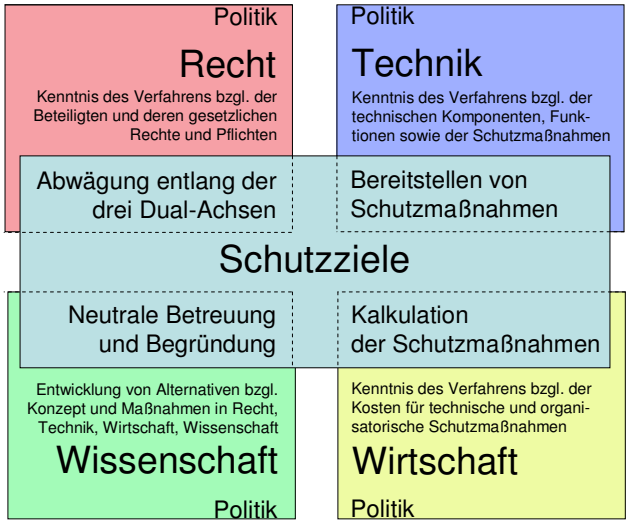
(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz im Sinne von § 3 Abs. 3 ist durch technische und organisatorische Maßnahmen sicherzustellen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. Sie müssen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

Schutzziele vermitteln Recht und Technik ohne einseitige Dominanz



Schutzziele als „Universalvermittler"



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

Schutzziele und Maßnahmen zu deren Umsetzung

- Sicherstellung von **Verfügbarkeit**
  Daten/Prozesse: Redundanz, Schutz, Reparaturstrategien
- Sicherstellung von **Integrität**
  Daten: Hash-Wert-Vergleiche
  Prozesse: Festlegen von Min./Max.-Referenzen, Steuerung der Regulation
- Sicherstellung von **Vertraulichkeit**
  Daten: Verschlüsselung
  Prozesse: Rollentrennungen, Abschottung, Containern
- Sicherstellen von **Transparenz durch Prüffähigkeit**
  Daten: Protokollierung
  Prozesse: Dokumentation von Verfahren
- Sicherstellen von **Nichtverkettbarkeit** durch Zweckbestimmung/-bindung
  Daten: Pseudonymität, Anonymität (anonyme Credential)
  Prozesse: Identitymanagement, Anonymitätsinfrastruktur, Audit
- Sicherstellen von **Intervenierbarkeit** durch Ankerpunkte
  Daten: Zugriff auf Betroffenen-Daten durch den Betroffenen
  Prozesse: SPOC für Änderungen, Korrekturen, Löschen, Aus-Schalter, Changemanagement,

Schutzbedarfe für „Person" - Definition normal, hoch, sehr hoch

Strukturelle Orientierung an BSI-Grundschutzdefinition(*), doch Wechsel der Perspektive von Geschäftsprozessen einer Organisation auf die Perspektive einer betroffenen Person:

- **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.

((*) https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30748/standard_1002_pdf.pdf, S. 49.)

Verfahrens-komponenten

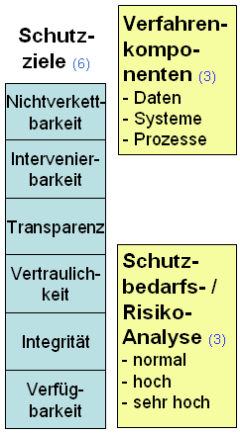
Ein Verfahren besteht aus drei zu betrachtenden Komponenten:

- Daten (und Datenformaten)
- IT-Systemen (und Schnittstellen)
- Prozesse (und adressierbare Rollen)

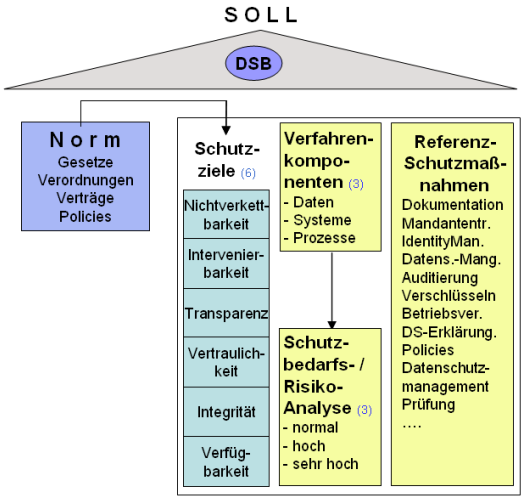
Das Standard-Datenschutzmodell (SDM)

- 6 Schutzziele, hinterlegt mit einem Maßnahmenkatalog!
- 3 Schutzbedarfsabstufungen, aus der Personenperspektive!
- 3 Verfahrenskomponenten!

Daraus lässt sich ein **Referenzmodell für 54 spezifische Datenschutzmaß-nahmen** entwickeln, gegen das sich jedes personenbezogene Verfahren skalierbar prüfen lässt!



Standard-Datenschutzmodell, Normen und Schutzmaßnahmen



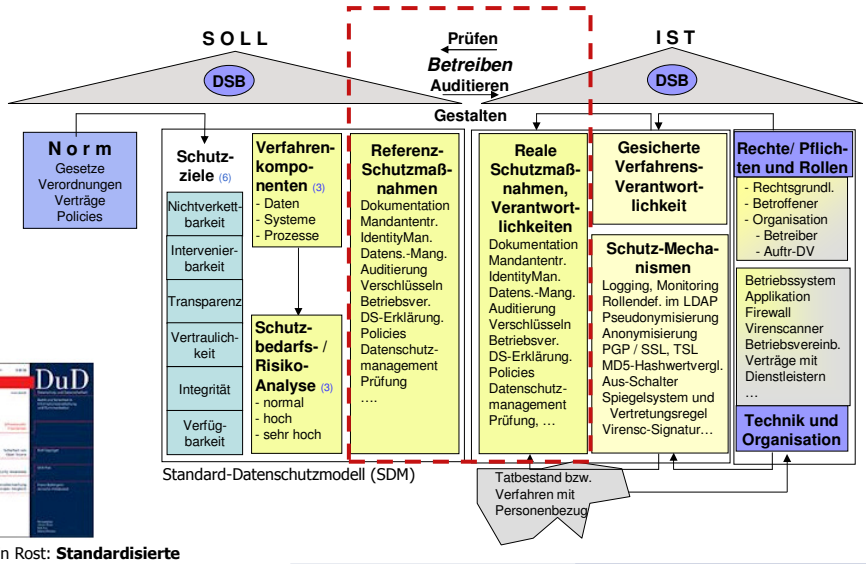
Standard-Datenschutzmodell (SDM)

Bock, Kirsten; Meissner, Sebastian: **Datenschutz-Schutzziele im Recht**; in: DuD 2012/06: 425-431.

ULD www.datenschutzzentrum.de

Standard-Datenschutzmodell: Prüfen und Gestalten

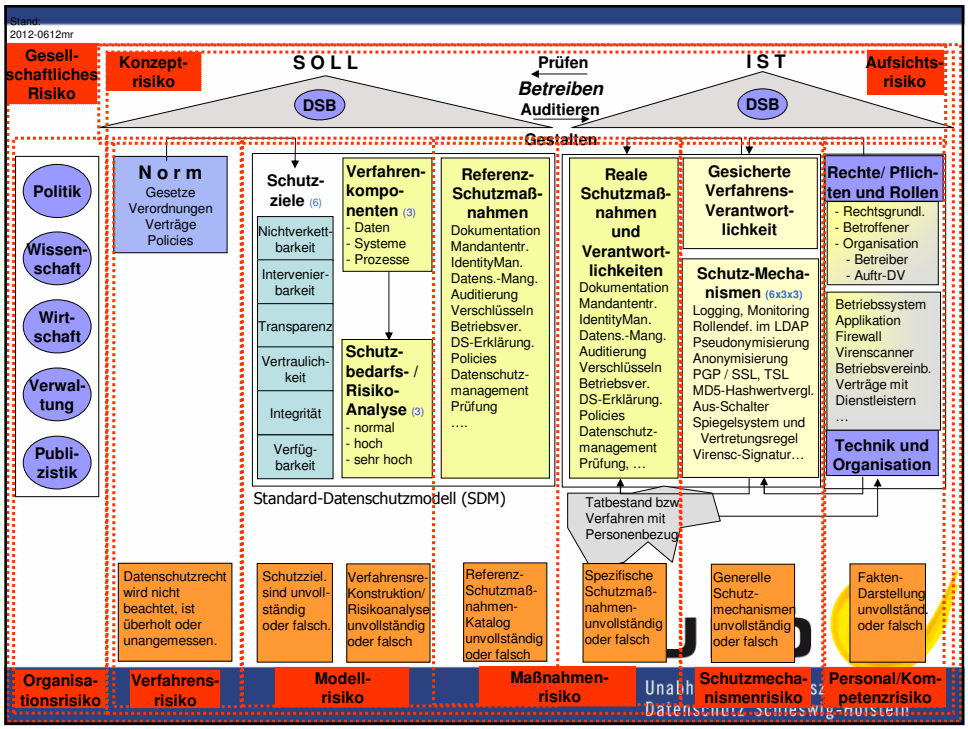
Stand:
2012-0612mr



Martin Rost: **Standardisierte Datenschutzmodellierung**;
in: DuD – 2012/06.: 433-438.

	Daten	Systeme	Prozesse
Verfügbarkeit	D1.1 Einschränkung von Lösch-/Veränderungsrechten D 1.2 Schutz vor Schadsoftware D 1.3 Backup der Daten	S 1.1: Schutz vor Schadsoftware S 1.2: Backup von Konfigurationen und Software S 1.3: Hardwareredundanz S 1.4: Ausweichräume, und -Netze	P 1.1: Vertretungspersonal P 1.2: Fähigkeit zur Aufgabenerledigung durch Dri (Vorbereitung Outsourcing) P 1.3: Ausweichprozesse, Amtshilfe
Vertraulichkeit	D 2.1: Einschränkung von Leserechten (für Datenverarbeiter, ggf. durch den Nutzer selbst) D 2.2: Protokollierung lesender Zugriffe D 2.3: Verschlüsselung der Daten D 2.4: Ende-zu-Ende-Verschlüsselung	S 2.1: Einschränkung von lesenden Zugriffsrechten auf IT-Systeme (z. B. Netztrennung durch Sicherheitsgateways) S 2.2: Verschlüsselung auf Systemebene (Festplatten, Datenbank)	P 2.1: Verpflichtung auf das Datengeheimnis (BDS P 2.2: Verschwiegenheitsvereinbarungen P 2.3: Geeignete Organisation bei der Vergabe von Zugriffsrechten („need-to-know“)
Integrität	D 3.1: Einschränkung von Schreib- und Änderungsrechten D 3.2: Protokollierung von schreibenden/ändernden Zugriffen D 3.3: Protokollierung geänderter Daten D 3.4: Nachberichtigung D 3.5: technische Integritätskontrollen (Signaturen/Hashes)	S 3.1: Einschränkung von schreibenden Zugriffen/Konfigurationmöglichkeiten auf IT-Systeme (z. B. Netztrennung durch Sicherheitsgateways) S 3.2: Regelmäßige Integritätsprüfungen/Audits	P 3.1: Detaillierte Planung von Verfahren und Verfahrensschritten P 3.2: Geordnete Zuweisung von Rechten und Roll P 3.3: Geordnete Änderung von Verfahren und Verfahrensschritten P 3.4: Regelmäßige Überprüfung
Nicht-Verkettbarkeit	D 4.1: Einschränkung von Verarbeitung-s-/Nutzungs- /Übermittlungsrechten für einzelne Daten D 4.2: Kennzeichnung der Zwecke auf Ebene der Daten D 4.3: Einschränkung von identifizierenden Daten; Pseudonymisierung D 4.4: Anonymisierung von Daten	S 4.1: Kennzeichnung der Zwecke auf Ebene des Systeme S 4.2: Trennung von Datenbeständen S 4.3: Einschränkungen von Verarbeitungs-, Nutzungs- und Übermittlungsmöglichkeiten (Funktionalitätseinschränkung) S 4.4: Trennung auf Systemebene (Software, Hardware; Mandantenfähigkeit)	P 4.1: Trennung auf Verfahrensebene P 4.2: Rechte + Rollenvergabe, ggf. an eine andere rechtliche Entität (z. B. Personalvertretung) P 4.3: Gewaltenteilung
Transparenz	D 5.1: Dokumentation der Datenfelder einschließlich Erforderlichkeit D 5.2: Protokollierung von Datenverarbeitungen mit Schutzbedarf zunehmender Detaillierungsgrad und Speicherdauer D 5.3: Integritätsschutz der Protokolle (separater Protokollierungsserver)	S 5.1: Dokumentation der Systeme (Hardware, Software, Algorithmen) S 5.2: Protokollierung von Konfigurationsänderungen S 5.3: zunehmende Kontrolldichte bei höherem Schutzbedarfen; automatisiertes Monitoring	P 5.1: Dokumentation des Verfahren und einzelner Prozesse (einschließlich beteiligter Organisationsei Rollen und Übermittlungen an Dritte) P 5.2: Dokumentation der Änderungsprozesse
Intervenierbarkeit	D 6.1: Schaffung notwendiger Datenfelder (z. B. für Gegendarstellungen)	S 6.1 Funktionalitäten in den Systemen für die Bearbeitung von Sperrungen, Widersprüchen, Beauskunftungen S 6.2 Funktionalitäten in den Systemen für die Umsetzung von weiteren Rechten Betroffener (z. B. Rufnummerunterdrückung, Pseudonyme Nutzungsmöglichkeit, etc.) S 6.3 Funktionalitäten für Betroffene, einzelne Betroffenenrechte direkt wahrzunehmen (z.B. Auskunftsportal, „Datenbrief“, Zusendung von Protokollen, eigene Änderungsmöglichkeiten) S 6.4 Steuerungsmöglichkeiten für einzelne Funktionen („Overrride“) bei automatisierten Einzelentscheidungen S 6.5 Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem	P 6.1: Organisation der Umsetzung der Betroffenen (Rechte + Rollen für Auskunft, Sperrungen) P 6.2: Organisation der Umsetzung der Betroffenen (Rechte und Rollen bei der Bearbeitung von Gegendarstellungen und Einwänden; Übersteuer automatisierter Einzelfallentscheidungen) P 6.3: Single Point of Contact für Datenschutzfrag

Thomas Probst: **Generische Schutzmaßnahmen für Datenschutz-Schutzziele**;



Vergleich der Prüfpraxis von Datenschutz und Datensicherheit IT-gestützter Verfahren:

- **bis zum Jahr 2000**
- **zwischen 2000 und 2010**
- **ab dem Jahr 2010**

Prüfpraxis
bis zum Jahr 2000

- Datenschutz
  - *zuständig*: DSB, primär juristisch orientiert;
  - *TO-Maßnahmen*: typisch orientiert Anhang §9 BDSG, punktuelle Forderungen sofern Fachkenntnisse des Prüfpersonals (Verschlüss., Pseudonym., Integr.-Checks);
  - *Prüfmethode*: keine standardisierte, häufig Checkliste
- Datensicherheit
  - *zuständig (faktisch)*: IT-Admin/DSB;
  - *TO-Maßnahmen*: kaum Unterschied zu Datenschutz, zusätzl.: Backupstrategien;
  - *Prüfmethode*: wie Datenschutz.
- Folgen:

  Datensicherheit und TO-Maßnahmen des Datenschutzes werden in der Praxis weitgehend ident gesetzt.
  DSB führt, weil er Organisations-Prüferfahrungen hat und beim Management Druck durch Anforderungen gem. Datenschutzrecht entwickeln kann.

Prüfpraxis
zwischen ca. 2000 und ca. 2010

- Datenschutz
  - *zuständig*: DSB, primär juristisch orientiert mit zunehmend verbessertem Technik-knowhow.
  - *TO-Maßnahmen*: Neu hinzu kommen PET-Maßnahmen zur Sicherstellung von Anonymität, Pseudonymität („nutzerkontrolliertes Identitätenmanagement").
  - *Prüfmethode*: Erste Anlehnungen an IT-Grundschutz, ITIL, CoBIT, QM, ISO27XXX, erste spezifische DS-Audits mit eigenem Kriterienkatalog.
- Datensicherheit
  - *zuständig*: IT-Sicherheitsbeauftragter
  - *TO-Maßnahmen*: Maßnahmenkatalog nach Feststellung des Schutzbedarfs sowie Risikoanalyse;
  - *Prüfmethode*: Risikoanalyse und -bearbeitung anhand Schutzziele (CIA) Abarbeiten von BSI-Grundschutz-Katalogen, Prozess-Gestaltung vornehml. nach ITIL, Controlling gem. IT-Sicherheitsmanagement;
- Folgen:

  Verhältnis von Dschutz und DSicherheit ist schlecht konturiert, zu Lasten des Dschutz. Das Thema DSicherheit ist im Management angekommen. Aufgrund besserer Methoden dominiert Sicht der DSicherheit weitgehend den TO-Dschutz.

Prüfpraxis
ab 2010

- Datenschutz
  - *zuständig*: DSB (der SiBe wird zum Dschutz-Risiko);
  - *TO-Maßnahmen*: neu: Dschutz-Schutzzielen und Maßnahmen;
  - *Prüfmethoden*: BSI-Grundschutz-Methodik, Dschutzmanagement
- Datensicherheit
  - *zuständig*: SiBe (der DSB wird zum Verbündeten gegenüber der Leitung aber zum Risiko bei den Sicherheitsmaßnahmen);
  - *TO-Maßnahmen*: standardisiert nach BSI-GS-Katalogen
  - *Prüfmethoden*: standard. gem. BSI-GS-Sicherheitscheck, ISO27XXX
- Folgen
  - Klare Separierung Dschutz und Dsicherheit über „Betreuung von Schutzzieltripel und Perspektive" möglich,
  - Gleichrangigkeit von Dschutz und Dsicherheit in Prüf-Systematik;
  - Dschutz hat spezif. Schutzmaßnahmen (uc-identitymanagement);
  - Dsicherheit hat spezif. gesetzliche Grundlagen (bspw. De-Mail, nPA, IT-Sicherheitsgesetz, IT-Sicherheitsleitlinie für die deutsche Verwaltung);
  - Grundrechtlich begründeter Primat des Datenschutzes (wg. Art. 1).

DSB-Konferenz
der Länder und des Bundes vom 13.3.2013 in Bremerhaven zum SDM

1. „Der Arbeitskreis Technik empfiehlt die Nutzung des Standard-Datenschutzmodells (SDM).
2. Der Arbeitskreis Technik empfiehlt die Entwicklung eines Katalogs mit Referenzmaßnahmen des technisch-organisatorischen Datenschutzes für das SDM.
3. Die Weiterentwicklung des SDM und des Maßnahmenkatalogs soll in einer Arbeitsgruppe des Arbeitskreis Technik und in Abstimmung mit der Datenschutzkonferenz erfolgen."

Vielen Dank für Ihre Aufmerksamkeit!

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Der Artikel zum Vortrag:
Martin Rost, 2013: **Eine kurze Geschichte des Prüfens**; in: BSI, Informationssicherheit stärken – Vertrauen in die Zukunft schaffen, Tagungsband zum 13. Deutschen IT-Sicherheitskongress, Gau-Algesheim, Secumedia-Verlag: 25-35

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein
Martin Rost
Telefon: 0431 988 – 1200
uld32@datenschutzzentrum.de
http://www.datenschutzzentrum.de/