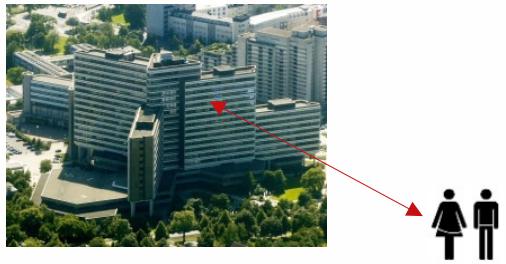


Datenschutz, Privacy und das Standard-Datenschutzmodell

Es ist vollkommen klar was zu tun ist

Martin Rost

Forum Privatheit

Berlin, 27.11.2015

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Agenda

1. Was meint „Datenschutz“?
   - Ein bißchen Theorie
2. Vorstellung des Standard-Datenschutzmodells
   - Operationalisierung von Schutzzielen
3. Das SDM benutzen

Quellen

„*Zivilisation heisst: Differenzierung.*“
(Niklas Luhmann / Sascha Lobo)

Datenschutz?
Privacy?
Typisches Beispiel für unterentwickelte juristische Begrifflichkeit

hieraus jedoch nicht. Im internationalen Verkehr werden sowohl 'privacy' als auch 'data protection' als Rechtsbegriffe verwendet.[77] Wie bereits festgestellt, ist das Schutzgut des Datenschutzes, die personenbezogenen Daten, leichter objektiv zu bestimmen als das Schutzgut der Privatheit.[78] Da der Datenschutz eine vergleichsweise neue Erscheinung bildet, wird sein Schutzgut darüber hinaus auch in internationalen Dokumenten häufig vorab definiert.[79] Als konkreter Rechtsterminus weist der Begriff ‚Datenschutz' daher vergleichsweise scharfe Konturen auf. Demgegenüber ist das Private ein wertbesetzter, schillernder Begriff und deshalb auch als Rechtsbegriff schwieriger zu handhaben.[80]

Stephanie Schiedermair, 2012: Der Schutz des Privaten als internationales Grundrecht, Mohr Siebeck, Lehrstuhl für Europarecht, Völkerrecht und Öffentliches Recht der Universität Leipzig: S. 18

Datenschutz das weitgehend unbekannte Wesen...

Datenschutz ist nicht mit Datenschutzrecht gleichzusetzen!

Denn das Datenschutzrecht reagiert auf einen (regelungsbedürftigen) Konflikt. Darf als geklärt unterstellt werden, worin genau dieser regelungsbedürftige Konflikt besteht?

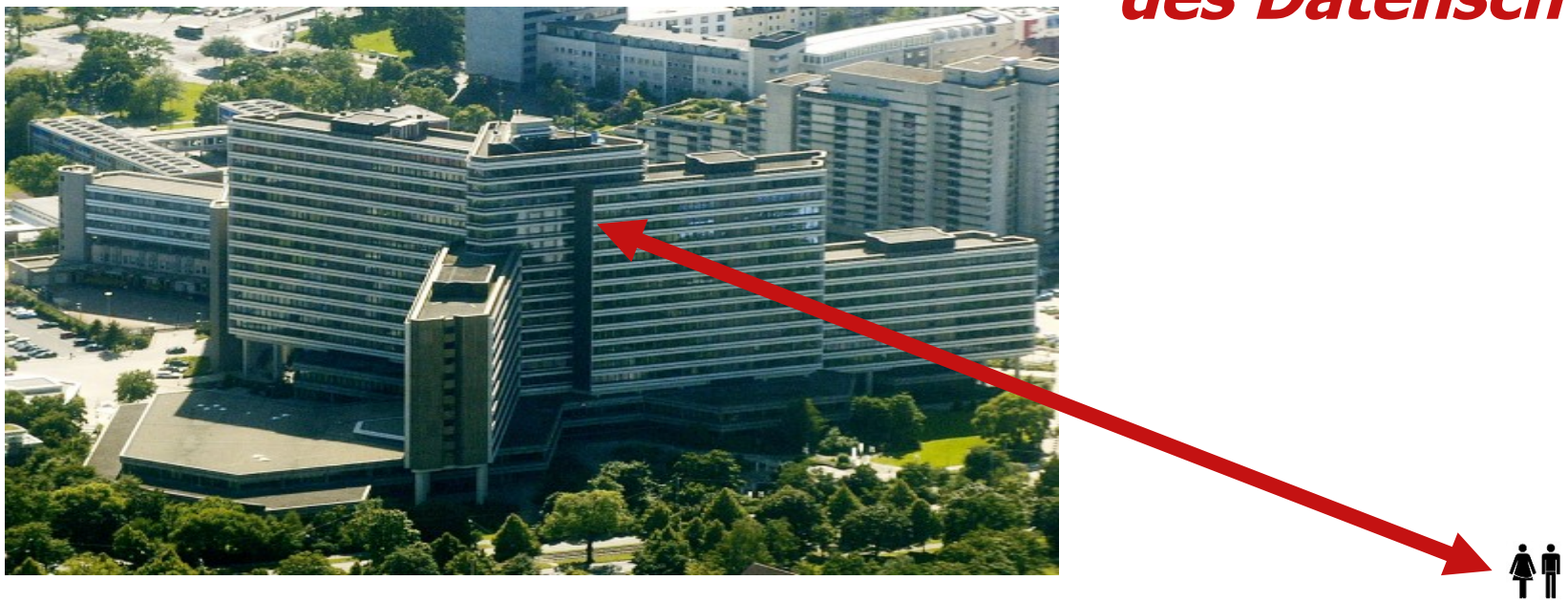
Operativer Datenschutz ist nicht mit den Maßnahmen der IT-Sicherheit gleichzusetzen!

Darf als geklärt gelten, wem der Schutz sicherheitstechnischer Maßnahmen - wie Verschlüsselung, Signieren, Anonymisieren - unmittelbar gilt? Dem Schutz der Behörde, dem Unternehmen, der Arztpraxis oder dem Schutz des Bürgers, des Kunden, des Patienten?

Die Institutionalisierung des Datenschutzes ergibt sich nicht aus einem (privaten?) Bedürfnis nach Privatheit.

Privatheit ist eine objektiv bestehende Struktur allein in einer modernen Gesellschaft. Darf als geklärt gelten, was unter „moderner Gesellschaft" zu verstehen ist? Ist Datenschutz schon deshalb obsolet, wenn Personen Privacy gleichgültig ist?

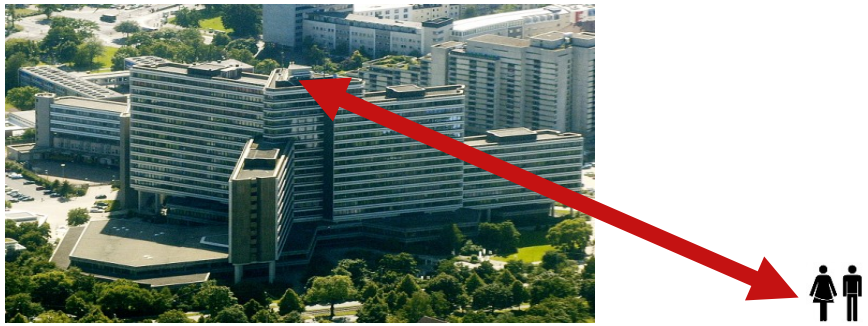
Objektbereich des Datenschutzes



Datenschutz beobachtet, thematisiert, beurteilt und gestaltet die Machtbeziehungen zwischen Organisationen und Personen...

... im Kontext einer modernen, d.h. funktional-differenzierten Gesellschaft.

Objektbereich des institutionalisierten Datenschutzes



Die Beziehungen zwischen Organisationen und Personen sind durch **Machtasymmetrien zu Gunsten von Organisationen** gekennzeichnet.

Die datenschutzrechtliche Beurteilung und Gestaltung dieser Machtasymmetrie durch Datenschutzaufsichtsbehörden geschieht anhand gesetzlicher Anforderungen, die aus Grundrechten abgeleitet sind und die Organisationen zu erfüllen haben.

Was sind Grundrechte?

Konventionell formuliert: Grundrechte sind Abwehrrechte des Bürgers gegenüber dem Staat und zugleich durch den Staat konstituiert, mit „Drittwirkung" auch auf Unternehmen.

Modernisiert verallgemeinert formuliert: **Grundrechte sind Abwehrrecht von Personen gegenüber Organisationen.**

Artikel 1 Grundgesetz

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.

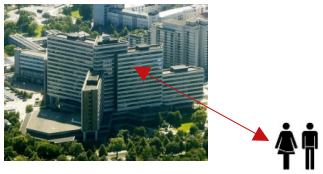
(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Artikel 2

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

„Volkszählungs-urteil" des BVerfG. von 1983



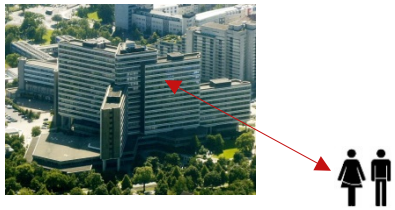
Zentrale Datenschutz-Figur: „Recht auf **informationelle Selbstbestimmung**"

(BVerfGE 65, 1 - Volkszählung (http://www.servat.unibe.ch/dfr/bv065001.html))

1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen *Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG* umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

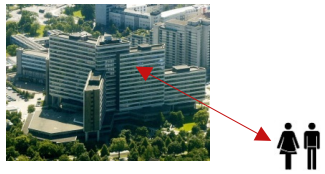
2. Einschränkungen dieses Rechts auf "*informationelle Selbstbestimmung*" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer *verfassungsgemäßen gesetzlichen Grundlage*, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

DER datenschutzrechtliche Grundsatz



Organisationen dürfen keine personenbezogene Daten verarbeiten PUNKT

„Verbot mit Erlaubnisvorbehalt“
(§4 Abs. 1 BDSG / §11 Abs. 1 LDSG-SH)

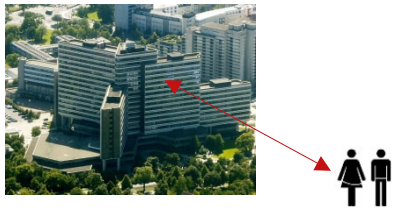


Voraussetzung einer ordnungsgemäßen Verarbeitung personenbezogener Daten

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit

- ein **Gesetz** die Verarbeitung regelt, was insbesondere für den öffentlichen Bereich gilt oder wenn
- eine **Einwilligung** vorliegt, was insbesondere im privaten Bereich der Fall ist. An eine Einwilligung sind folgende Bedingungen geknüpft:
  - Bestimmung des Zwecks,
  - Freiwilligkeit,
  - Informiertheit und Bestimmtheit der Verarbeitung,
  - abschließende Bestimmung der Empfänger.

Zum Verhältnis von Datenschutz und IT-Sicherheit



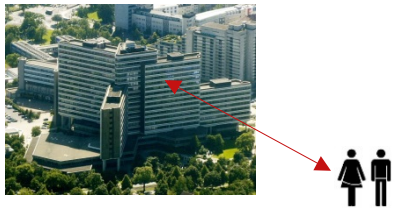
IT-Sicherheit unterstellt:

Jede Person kann ein Angreifer sein!
Die Person muss deshalb nachweisen, dass sie kein Angreifer ist.

Datenschutz unterstellt:

Jede Organisation ist ein Angreifer!
Die Organisation muss deshalb nachweisen, dass sie kein Angreifer ist, u.a weil sie sich an die Regeln/Gesetze hält und bei all dem ihre Verfahren und Prozesse gesichert beherrscht.

Krypto-szenarisch gesprochen gilt für Datenschutz

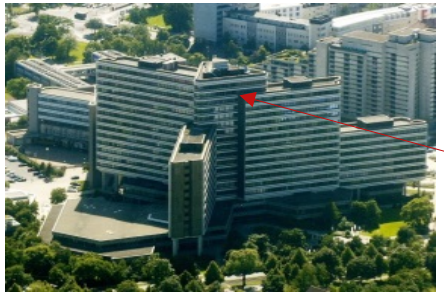


Bob ist der Angreifer!

Sicherheit? Datenschutz?

- **Herstellen von Betriebssicherheit („Safety")**
  Gilt dem Schutz von technischen Funktionen durch Ausfälle oder menschlichem Versagen, aber auch durch Verschleiß und Bedienungsfehler.
- **Herstellen von IT-Sicherheit („Security")**
  Gilt dem Schutz vornehmlich von Geschäftsprozessen von Organisationen vor zielgerichteten und *böswilligen Angriffen* von innen und außen. („IT-Grundschutz" des BSI)
- **Herstellen persönlicher IT-Sicherheit („Personal Security")**
  Gilt dem technischen gestützten *Selbstschutz* von Einzelpersonen vor böswilligen Angriffen durch externe Hacker.
  (personal firewall, Virenscanner, Login)
- **Herstellen von „Privacy"**
  Gilt dem Schutz von Betroffenen vor Organisationen mit Selbstschutzaktivitäten(?) auf Seiten der Betroffenen.
  (Nutzung von Verschlüsselung oder Anonymisierungsproxy)
- **Herstellen von Datenschutz**
  Gilt dem grundrechtlich verankerten Schutz von Betroffenen vornehmlich vor *Aktivitäten* durch (auch ordnungsgemäß agierende) *Organisationen* mit Schutzvorkehrungen für Betroffene auf Seiten der Organisationen.

Zum Verhältnis Organisation – Person



Organisationsformen

- öffentliche Verwaltung
- private Unternehmen
- IT-Infrastruktur-Provider (bspw. Access-, Suchmaschinen-, Mail-, Socialnetwork-Betreiber);
- Praxen / Institute
- Wissenschaftsorganisationen

- Arbeitgeber und totale Institutionen (bspw. auch Schule, Krankenhaus, Kirche, Militär, Verein, Gefängnis, …)

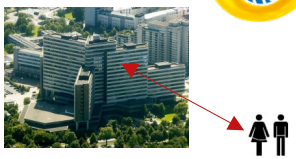
Personen-Rollen

- Bürger
- Kunde
- Nutzer

- Patient, Mandant, Klient
- Individuum, Subjekt, Mensch

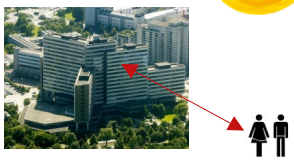
- Mitarbeiter und Mitglied (Schüler, Patient, Gefangener, Soldat, …).

Gesellschaft
Organisation und Person



- **Die Anforderung nach Konditionierung der Machtasymmetrie ist** keine, die unmittelbar mit einer antrophologisch verstandenen, überhistorisch a-sozialen Persönlichkeitsausstattung „DES MENSCHEN" begründbar ist und politisch und persönlichkeitsrechtlich als liberale Imagination zu Autonomie, Individualität, Freiheit, „informationeller Selbstbestimmung" usw. daherkommt, sondern sie ist zunächst **eine Reaktion auf die Kontingenz- und Risikoquellen moderner Gesellschaften, mit Folgen für die Personen- und Privatheitskonzepte einer solcher Gesellschaft.**
- Personen moderner Gesellschaften, die in den Rollen als Bürger, Kunde oder Patienten *auftreten müssen*, haben diese Rollen, die Autonomie und Privatheit verlangen und Individualität konstituieren, nicht aus freien Stücken gewählt. **Die Rollen des Bürgers, des Kunden, des Subjekts usw. mit ihren Zwängen zur informationellen Selbstbestimmungen werden jeder *Person* allgemein *gesellschaftlich zugewiesen* und im Umgang mit *Organisationen konkret geformt***.

Gesellschaft
Organisation und Person



Das was als „Personen-Konzept" von Privatheit, Freiheit, Individualität, informationeller Selbstbestimmung funktional-differenziert gesellschaftlich erzeugt wird und von Personen zu erfüllen ist („**Zwang zur Individualität**", Meutert 2002), wird zugleich **von Organisationen notorisch unterlaufen:**

Etablierte Unternehmen haben kein Interesse am Markt (Monopolisierung), Sicherheitsbehörden kein Interesse an Gewaltenteilung (Dominanz der Exekutive), etablierte Forschungsinstitute kein Interesse an freien Diskursen (Theorie und Methoden-Verbote, Orientierung an Reputation, anstatt Funktion). **Aus Organisationssicht bedeuten informationell selbstbestimmte Kunden, Bürger und Patienten... erhöhte Risiken für Organisationen.**

Organisationen untergraben notorisch die Kontingenzquellen moderner „funktional differenzierter" (Luhmann) Gesellschaften. **Organisationen nutzen IT, um die Risiken des Marktes (Kunden), der öffentlichen Ordnung (Bürger), der freien Diskurse (Subjekte) zu ihren Gunsten zu verringern.**

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

Geltungsanforderungen an vernünftige Kommunikationen

Habermas (1981, Theorie des kommunikativen Handelns) unterscheidet vier Arten von Geltungsansprüchen sinnhafter Kommunikationen, die nicht aufeinander zurückgeführt werden können:

Verständlichkeit

Der Sprecher unterstellt das Verständnis der gebrauchten Ausdrücke. Bei Unverständnis wird zur Explikation durch den Sprecher aufgefordert.

Wahrheit

Bezüglich des propositionalen Gehalts der Sprechakte wird Wahrheit unterstellt. Wird diese bezweifelt, muss ein Diskurs klären, ob der Anspruch des Sprechers zurecht besteht.

Richtigkeit

Die Richtigkeit der Norm, die mit dem Sprechakt erfüllt wird, muss anerkannt werden. Auch dieser Geltungsanspruch ist nur diskursiv einlösbar.

Wahrhaftigkeit

Die Sprecher unterstellen sich gegenseitig Wahrhaftigkeit (Aufrichtigkeit). Erweist sich diese Antizipation (Voraussetzung) als unhaltbar, kann der Hintergrundkonsens nicht mit dem unwahrhaften Sprecher selber wiederhergestellt werden.

Würde wird kommunikativ konstituiert

- Eine vernünftig gelingende Kommunikation im Sinne von Jürgen Habermas „Geltungsanforderungen an eine vernünftige Rede" setzt voraus, dass die **Informations- und Kommunikationstechnik, die Organisationen bereitstellen und nutzen, diese Geltungsanforderungen nicht unterlaufen**.

- **Die Anforderungen des Datenschutzes an Organisationen ergänzen diese Geltungsanforderungen auf operativer Ebene.**

- Nur wenn diese Geltungsanforderungen faktisch eingelöst werden, kann sich **Würde des Menschen kommunikativ konstituieren**.

Politische Exekutive hält aktuell den Grundrechteschutz für zu stark

Merkel auf dem IT-Gipfel: Datenschutz darf Big Data nicht verhindern

heise online 19.11.2015 17:13 Uhr – Stefan Krempl

Bundeskanzlerin Angela Merl

Bundeskanzlerin Ange
Datensparsamkeit im I
den entsprechenden K

IT-Gipfel: Gabriel plädiert für Datensouveränität statt Datenschutz

heise online 19.11.2015 12:00 Uhr – Stefan Krempl vorlesen

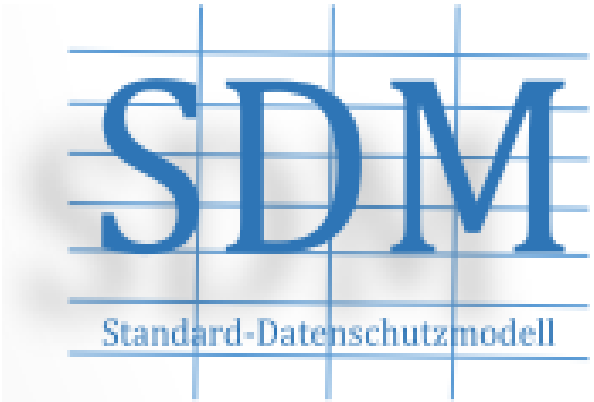
Sigmar Gabriel spricht zur Eröffnung des IT-G

"Wir brauchen ein anderes Verstär
Sigmar Gabriel zur Eröffnung des S
zum Geschäftsmodell Big Data.

EU-Datenschützer warnt vor Big-Data-Diktatur

heise online 20.11.2015 13:15 Uhr – Stefan Krempl vorlesen

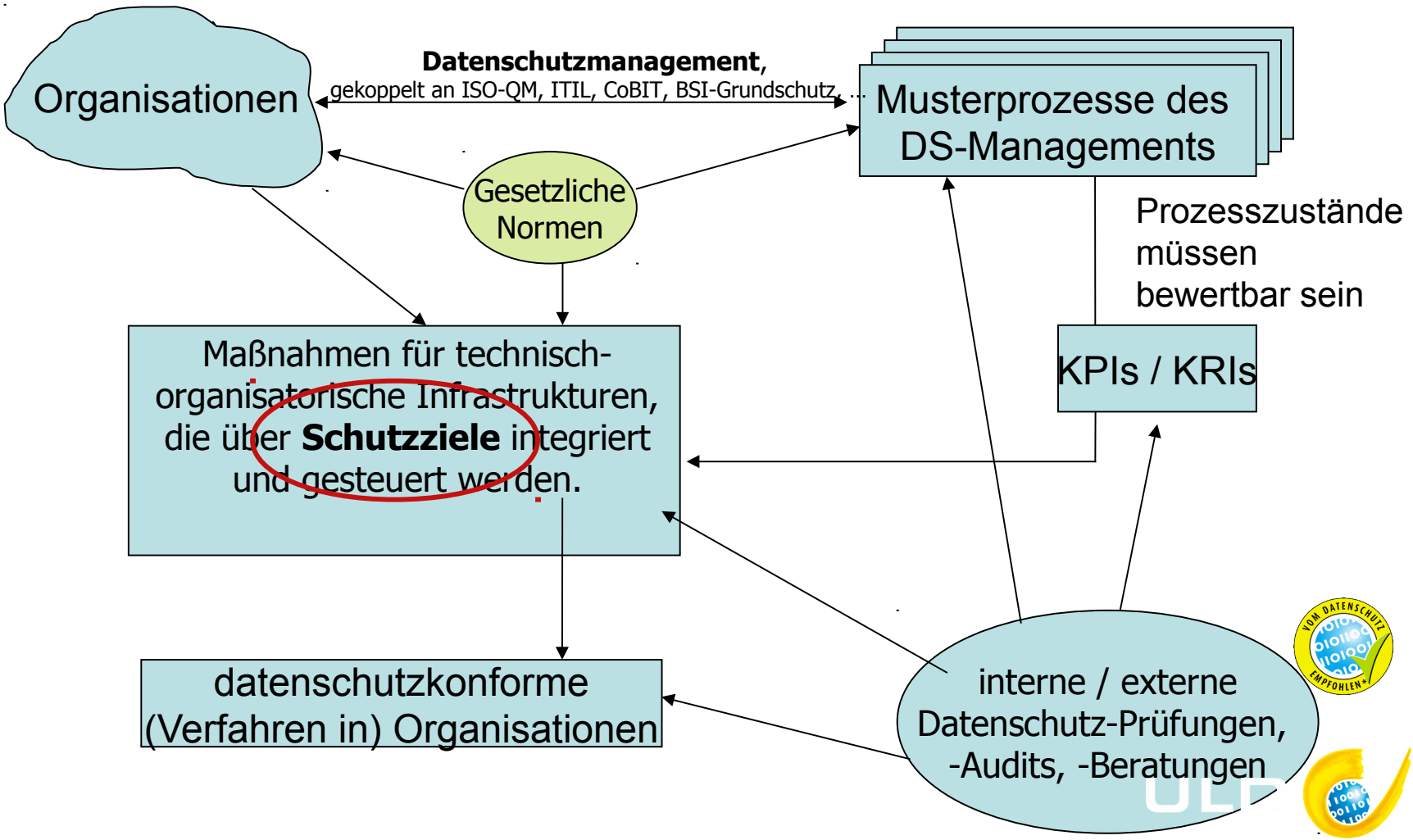
Europa dürfe nicht unkritisch "datengetriebene Technologien und Geschäftsmodelle" importieren, betont der EU-Datenschutzbeauftragte Giovanni Buttarelli. Auch bei Big Data müssten Grundrechte gewahrt bleiben.



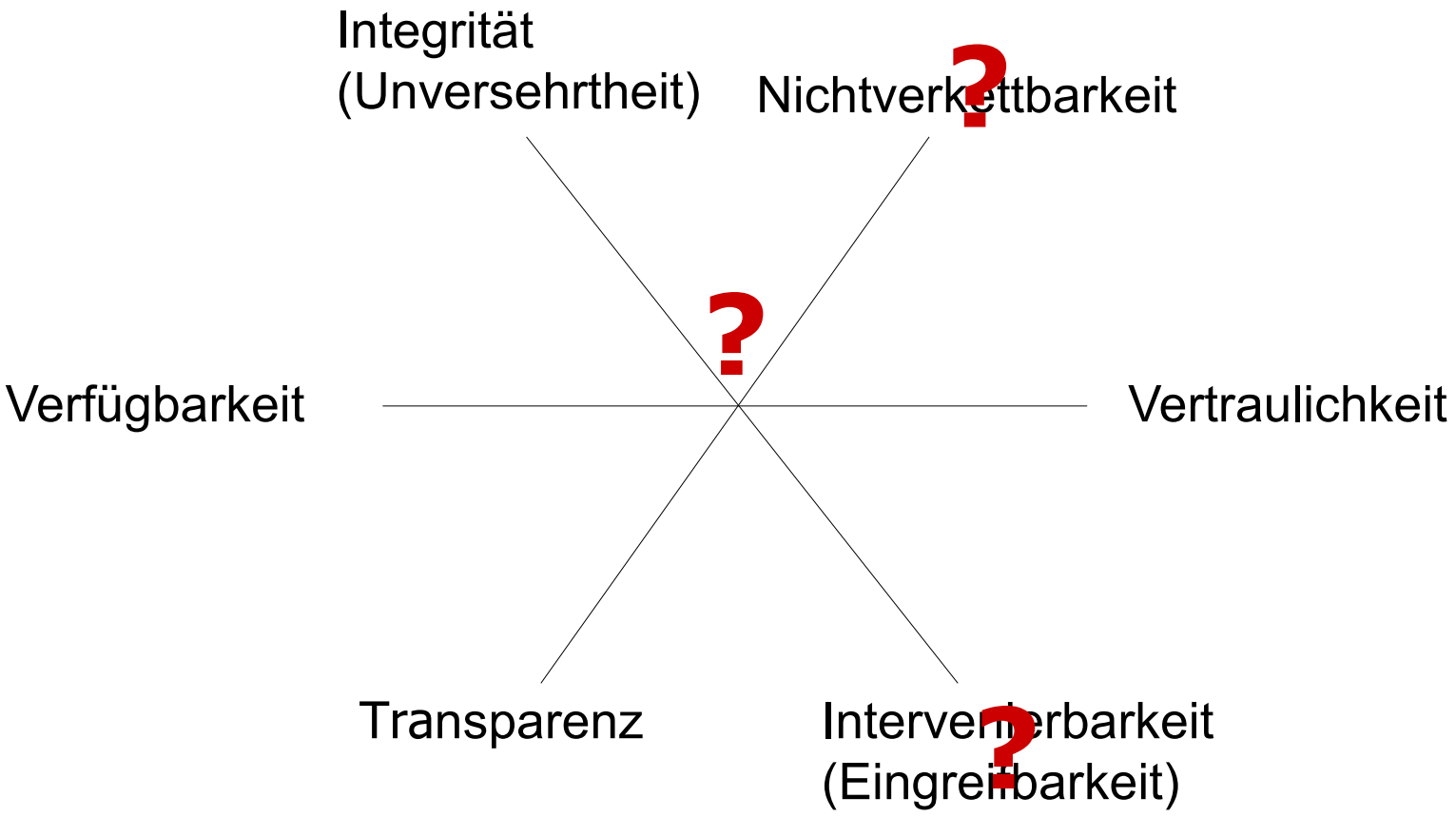
Das Standard-Datenschutzmodell (SDM)

Normativer Ausgangspunkt des SDM sind Schutzziele

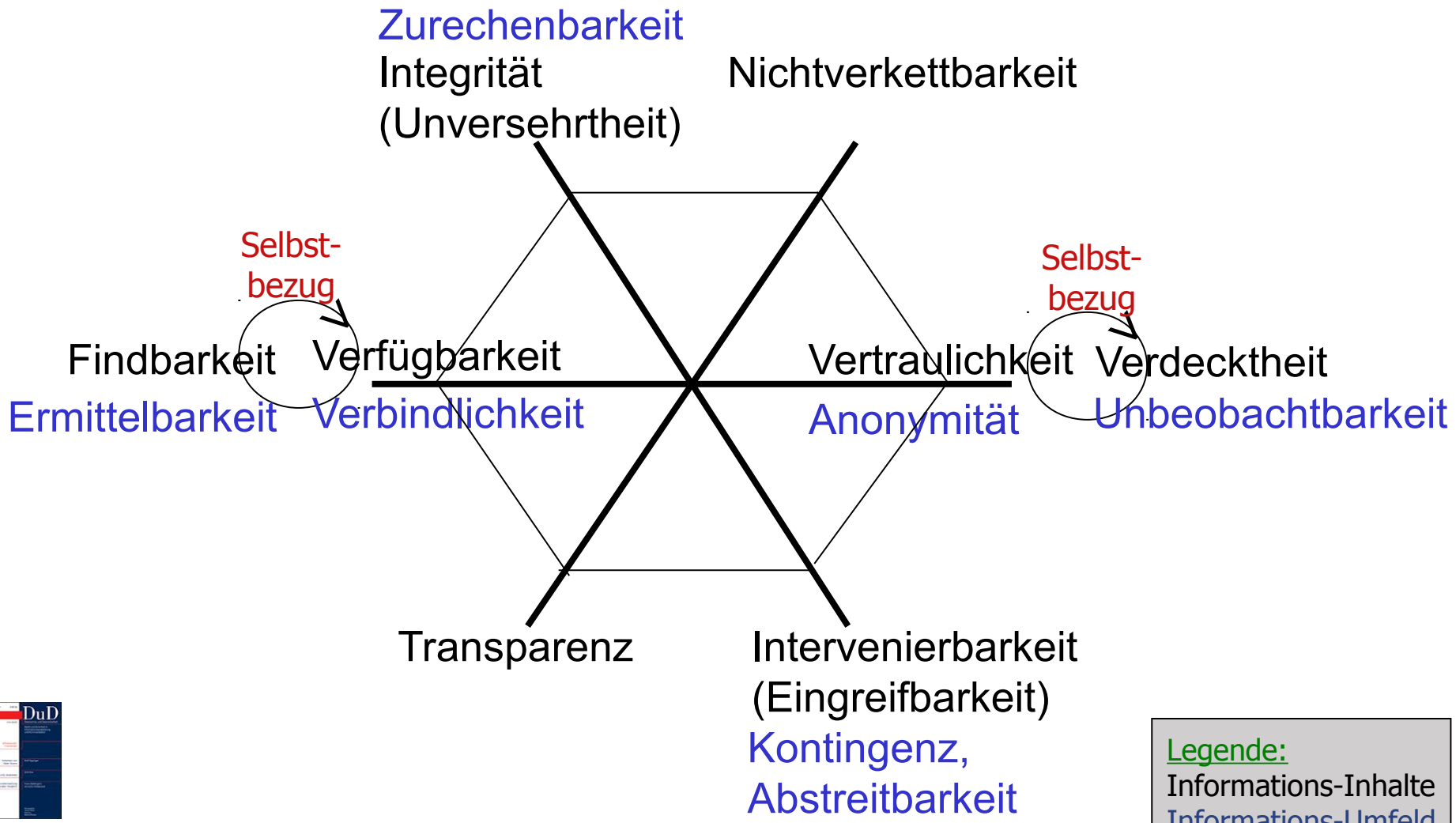
Big Picture
Prozesse, DS-Management, Schutzziele, KPI/KRI



Schutzziele Systematik



Schutzziele
Systematik, vollständig



Legende:
Informations-Inhalte
Informations-Umfeld

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

Schutzziele im LDSG-SH, § 5

Organisationen müssen gewährleisten, dass (...)

„Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können (**Verfügbarkeit**),

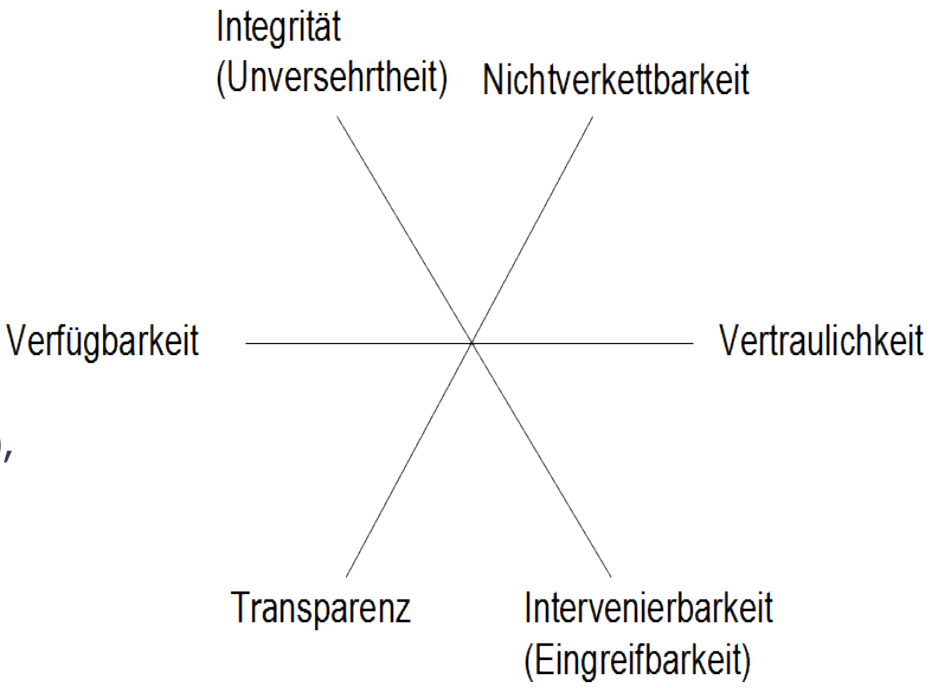
Daten unversehrt, vollständig, zurechenbar und aktuell bleiben (**Integrität**),

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**).“



Vermittlung von Soll und Sein durch Schutzziele

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

Wie lässt sich dieses Schutzzielekonzept skalierbar operationalisieren?

Mapping Schutzziele und BDSG

Tabelle: Zuordnung der gesetzlichen Vorgaben zu den Gewährleistungszielen.

Datenspar-samkeit	Verfügbar-keit	Integrität	Vertrau-lichkeit	Nichtver-kettbarkeit	Transpa-renz	Intervenier-barkeit
	Nr. 7 der Anlage zu § 9	Nr. 1-6 der Anlage zu § 9	Nr. 1-6 so-wie 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

Aus: SDM-Handbuch, V 0.9

SDM
Schutzbedarfsdefinition

Normal: Schadensauswirkungen sind begrenzt und überschaubar und etwaig überzogene Aktivitäten einer Organisation und 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.

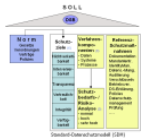
sehr hoch: Die Schadensauswirkungen nehmen ein unmittelbar existentiell bedrohliches, katastrophales Ausmaß für Betroffene an, wenn eine Organisation überzieht.

(Quelle: „Das Standard-Datenschutzmodell“, V0.9, Oktober 2015)

SDM
Verfahrenskomponenten

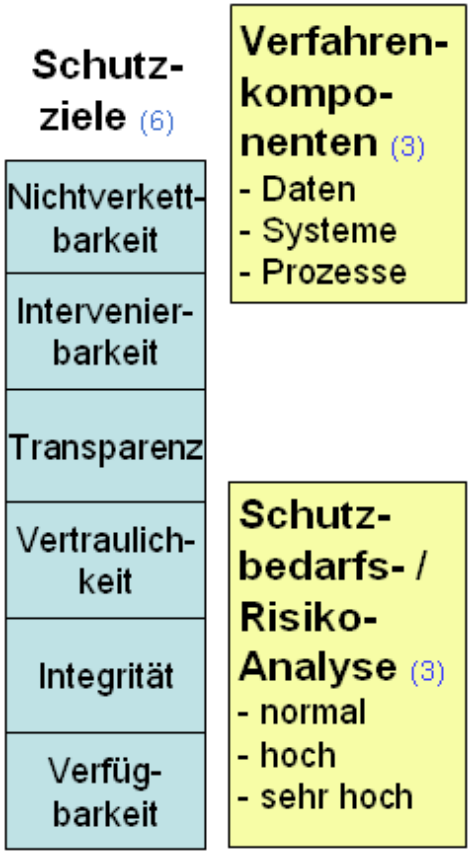
Ein personenbezogenes Verfahren besteht aus drei zu betrachtenden Komponenten:

- Daten (und Datenformaten)
- IT-Systemen (und Schnittstellen)
- Prozessen (und adressierbaren Rollen)



Das Standard-Datenschutzmodell (SDM)

- **6 Schutzziele, hinterlegt mit Schutzmaßnahmen-Katalog (plus Datensparsamkeit als generisches „Superschutzziel")**
- **3 Schutzbedarfsabstufungen, aus der Personenperspektive**
- **3 Verfahrenskomponenten**



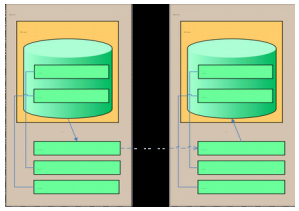
Das ergibt ein **Referenzmodell für 6x3x3 (54) spezifische Datenschutzmaßnahmen**, gegen das sich jedes personenbezogene Verfahren standardisiert prüfen lässt!

Maßnahmen zur Sicherung der Verfügbarkeit

Verfügbarkeit:
Informationen sind dort und dann zugänglich,
wo und wann sie von Berechtigten gebraucht werden.

Schutz von Verfügbarkeit: Gewährleisten von Funktionalität gegen vorsätzliche oder versehentliche Einschränkung, z.B. durch

- **Redundanz** (Daten, Systeme, Prozesse)
  - Backup von Daten und Systemen
  - Vertretungsregelungen



www.openclipart.org

Maßnahmen zur Sicherung der Integrität

Integrität: Informationen sind richtig, vollständig und aktuell oder aber dies ist erkennbar nicht der Fall.

Schutz von Integrität:
Verhindern von unberechtigter Manipulation oder Datenverlust, z.B. durch

- **Prüfsummen**, fehlerkorrigierende Codes
- Einschränkung von Schreibrechten
- **Definition von Soll/Ist-Zuständen** bei Prozessen

Erkennen von Manipulationen durch

- Zeitstempel
- Protokolleinträge
- Signaturen und Prüfsummen
- Überprüfung von Soll-Ist-Werten

www.openclipart.org

Maßnahmen für Vertraulichkeit

Vertraulichkeit:
Informationen dürfen nur Berechtigten bekannt werden.

Schutz von Vertraulichkeit:
Verhindern von unberechtigter Kenntnisnahme, z.B. durch

- **Verschlüsselung** von Daten (Kryptographie)
- Verstecken von Daten (Steganographie)
- **Zugriffsbeschränkungen** durch Authentisierung- und Autorisierung (Rollenkonzept)

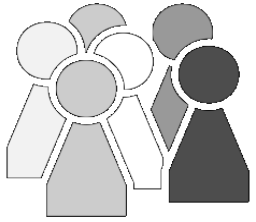
```
-----BEGIN PGP-----
0IxWZHhKYoECwCBeIweKU+0Ed
m068SB4ADeGGCtd+eacjDT5Ig
TdwAypl8+WOFYxTVEXbqOqjoW
mY4T9zuoSC5e
=lu9g
-----END PGP-----
```

Maßnahmen zur Sicherung der Nicht-Verkettbarkeit

Nicht-Verkettbarkeit: Ein personenbezogenes Verfahren darf nur für den bestimmten Zweck verwendet werden.

Sicherung von Nicht-Verkettbarkeit:

- **Pseudonymisierung / Anonymisierung** von Datenbeständen und Kommunikationsbeziehungen
- **Trennung von Verfahren** durch Trennung von Datenbeständen, IT-Systemen (Hardware/Software) und Prozessen.



www.openclipart.org

Maßnahmen zur Sicherung der Intervenierbarkeit

Intervenierbarkeit: Ein personenbezogenes Verfahren muss verändert werden können.

Sicherung von Intervenierbarkeit:

- Operative Umsetzung von Betroffenenrechten: **Einsichtnahme, Korrigieren, Sperren und Löschen**
- Nutzen eines reifen **Changemanagements** für
  - Störungen
  - Problembearbeitungen
  - strukturelle Änderungen einer Organisation

Maßnahmen zur Sicherung der Transparenz

Transparenz: Ein Verfahren erfüllt prüfbar die datenschutzrechtlich bestehenden Anforderungen.

Sicherung von Transparenz:

- **Dokumentation** von Verfahren, d.h. der Datenbestände, der IT-Systeme sowie der technischen Funktionen und organisatorischen Regelungen.
- **Protokollierung** der Prozesse

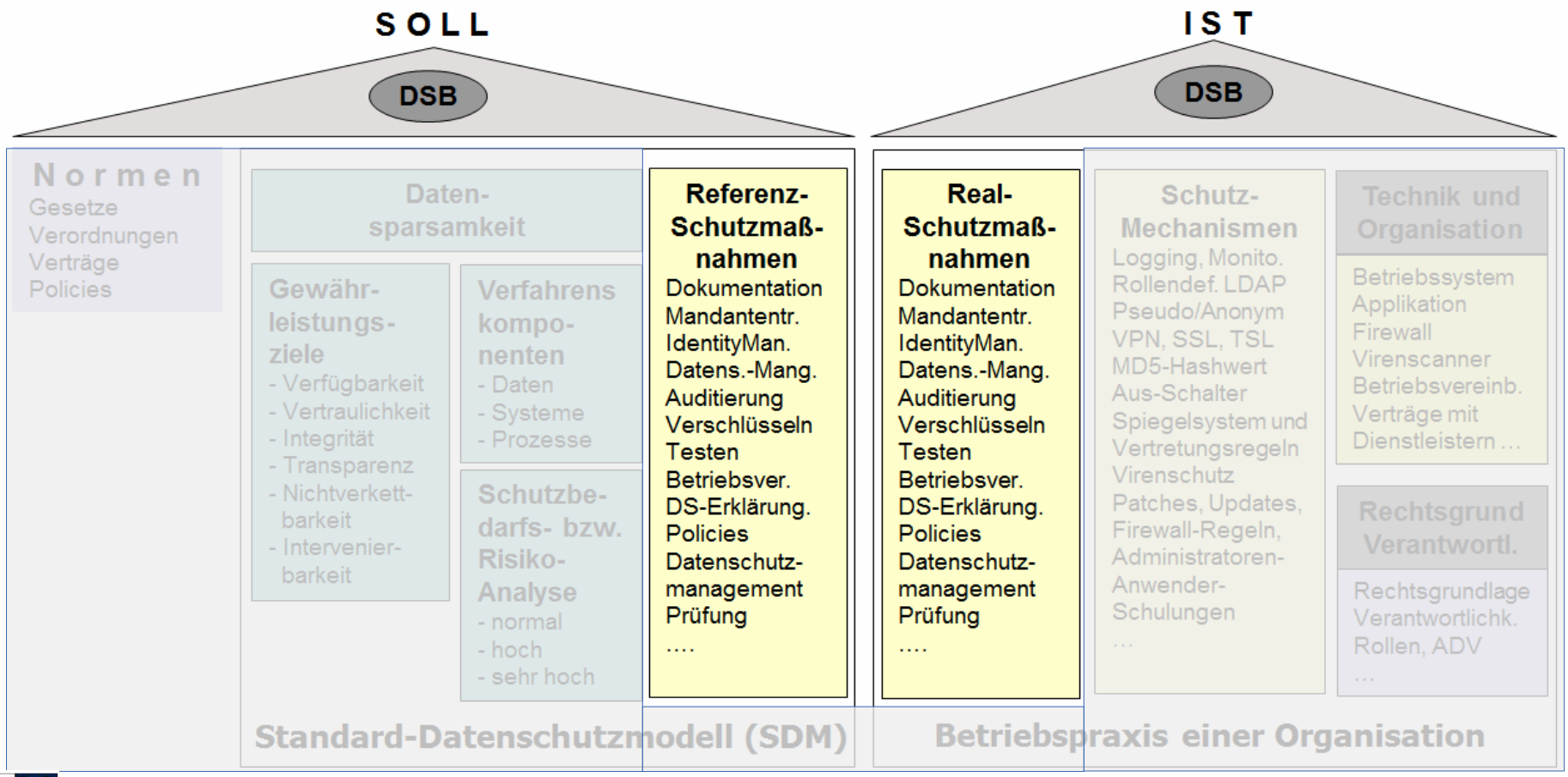
Beispiel Protokollierung

- **Zweck eines Protokolls:** Nachweis ordnungsgemäßer, rechtmäßiger Funktionenalität eines personenbezogenen Verfahrens entlang einer Prozesskette in einer Organisation. Ein Protokoll muss Antwort geben können auf die Frage: Wann hat wer welche Aktivität in oder mit der Organisation durchgeführt?
- **Inhalt eines Protokolls ist dreistellig:**
  - Zeitstempel (Auflösung? zertifizierter Zeitstempel? systemeigener Zeitserver?)
  - Ausführende Instanz (Client, Server, Programm, Admin, Sachbearbeitung?)
  - Eindeutiger Bezeichner der Aktivität
- **Protokollierungsebenen eines Verfahrens:**
  - Anwendungsebene Sachbearbeitung: Datenbearbeitung
    - Achtung: *Generell keine Verhaltens- und Leistungskontrolle!*
  - Anwendungsebene Administration: Installation, Änderungen der Konfiguration
    - Achtung: *Verhaltenskontrolle der Admins bei besonders kritischen Aktivitäten*
  - Installation, Konfiguration, Administration Hardware, OS, DB, Schutzmaßnahmen
    - Achtung: *Differenzierung der Admintätigkeiten*, nicht alles muss root machen!
  - Aktivitäten an Schnittstellen bei Datenübertragungen
    - Wenn Datenübertragung über mehrere unabhängige Organisationseinheiten hinweg: *Anfordern und Abspeichern von Quittungen der beteiligten Instanzen*

Datenschutz-gerechte Protokollierung: Was heisst das?

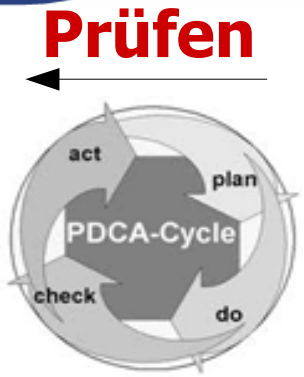
- **Protokolldaten müssen verfügbar sein**
  - Backup & Restore-Konzept auch für Protokolldaten
  - Link zw. Produktionsdaten und Protokolldaten
- **Protokolldaten müssen integritätsgesichert gespeichert sein**
  - Validität und Reliabilität von Protokolldateneinträgen
  - Signieren von Protokolldaten
  - Betrieb eines dedizierten Protokollierungsservers
- **Protokolldaten müssen vertraulich gespeichert und übermittelt werden**
  - Verschlüsselung von Protokolldaten
  - Zugriffsreglung auf Protokolldaten
- **Protokolldaten müssen transparent sein**
  - Dokumentation der Protokollierung
- **Protokolldaten dürfen nicht verkettbar sein**
  - Trennung der Protokolldatenbeständen
  - Protokolldaten müssen beurteilt werden und es müssen bei Abweichungen auch Konsequenzen gezogen werden
- **Protokolldaten müssen intervenierbar sein**
  - Löschen

Fokus einer Datenschutzprüfung mit SDM



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

Datenschutz-management mit SDM



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.
IdentityMan.
Datens.-Mang.
Auditierung
Verschlüsseln
Testen
Betriebsver.
DS-Erklärung.
Policies
Datenschutz-management
Prüfung
....

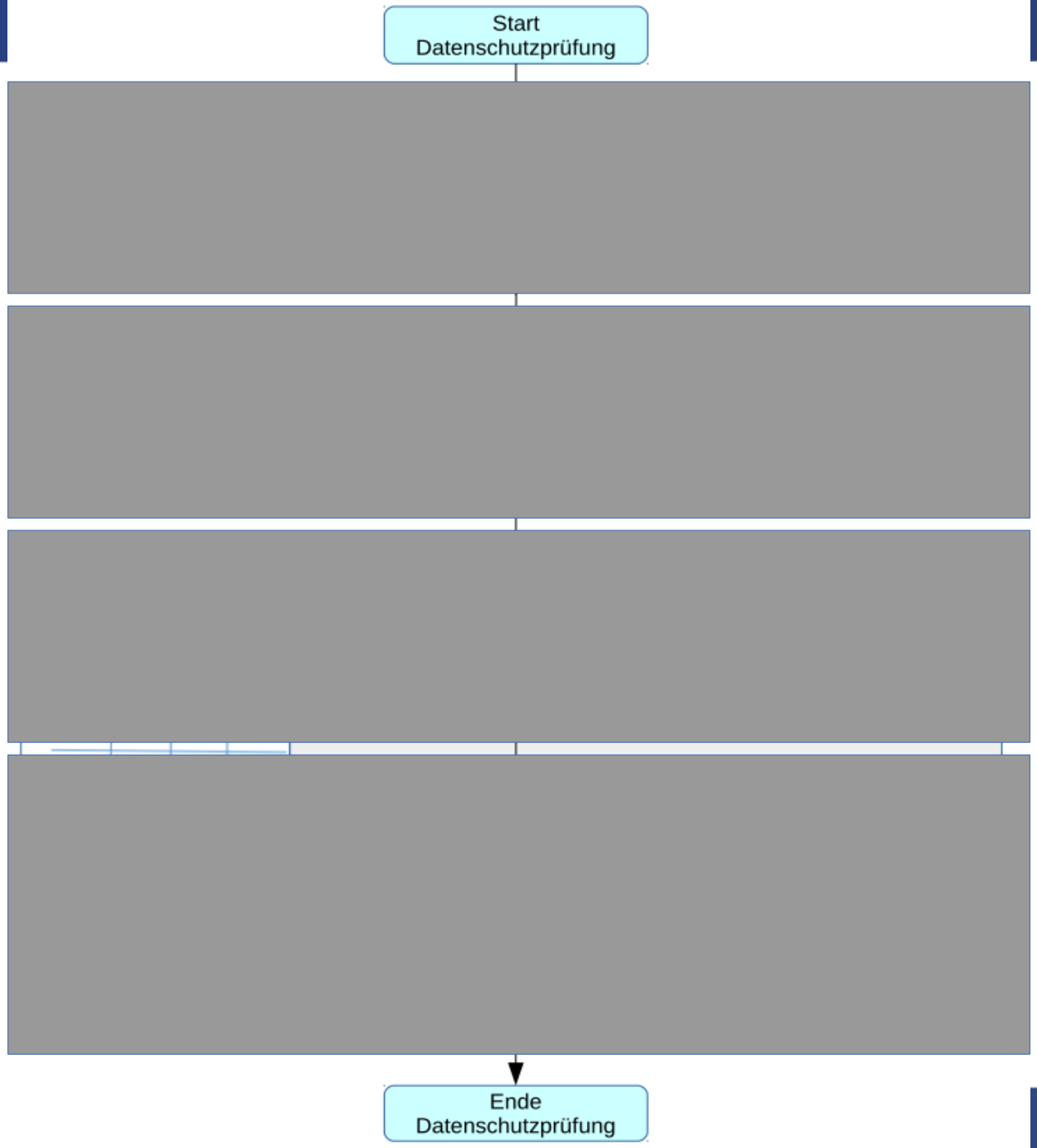
Schutz-Mechanismen
Logging, Monito.
Rollendef. LDAP
Pseudo/Anonym
VPN, SSL, TSL
MD5-Hashwert
Aus-Schalter
Spiegelsystem und
Vertretungsregeln
Virenschutz
Patches, Updates,
Firewall-Regeln,
Administratoren-
Anwender-
Schulungen
...

Technik und Organisation
Betriebssystem
Applikation
Firewall
Virenscanner
Betriebsvereinb.
Verträge mit
Dienstleistern ...

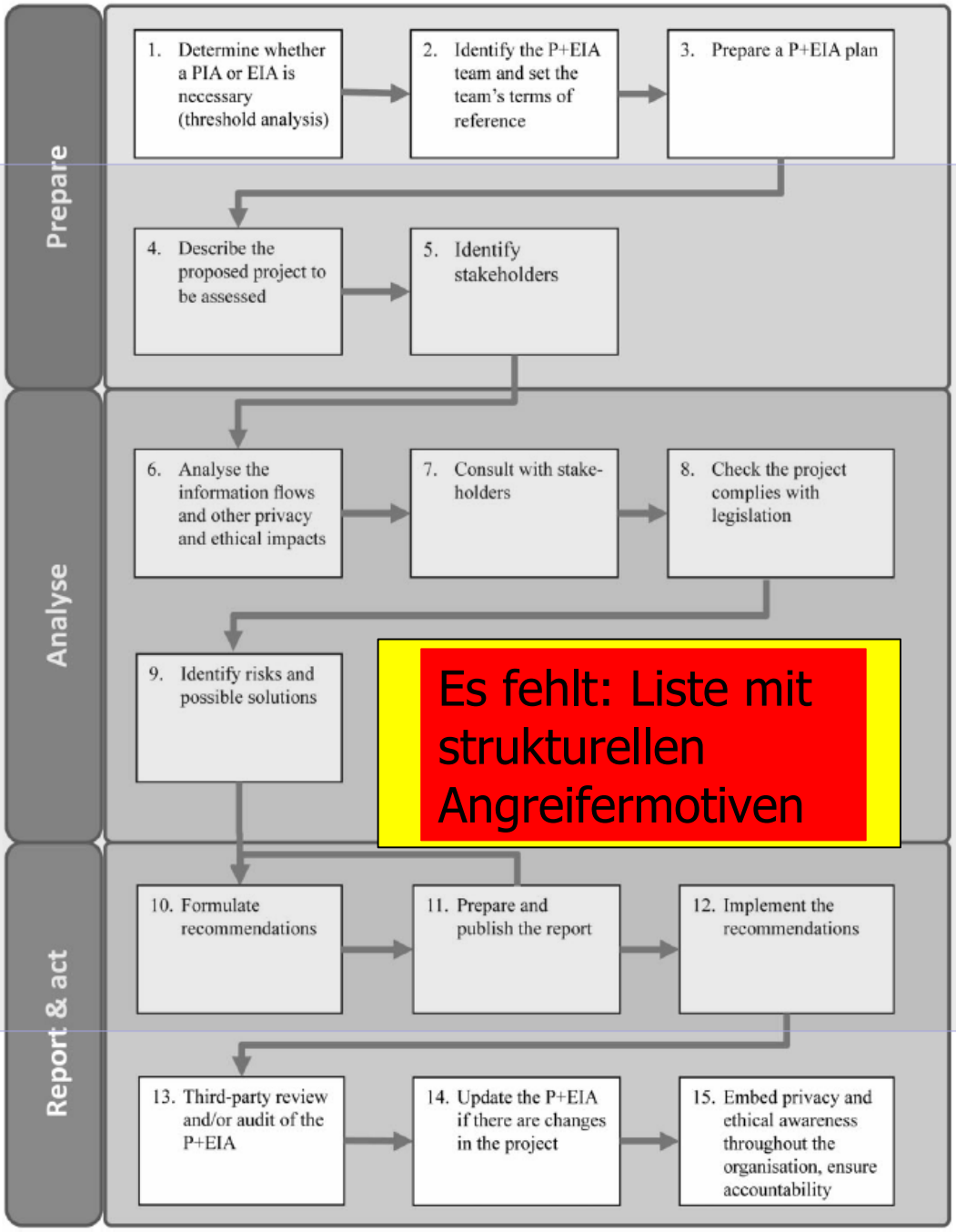
Rechtsgrund Verantwortl.
Rechtsgrundlage
Verantwortlichk.
Rollen, ADV
...

Betriebspraxis einer Organisation

Phasen einer Datenschutz-prüfung



PIA
(Wright/Friedewald 2013)



← Verfahrensbeschreibung einschl. verantwortliche Stelle, Prüfplanung

← Identifikation von Daten und Datenflüssen, Rechtsgrundlagen

← Schutzziele und Schutzmaßnahmen

← Sicherheitskonzept und Umsetzung

SDM

← Review des PIA und Fortschreibung

(Wright / Friedewald 2013: 763)

Status SDM 2015

heise online > News > 2015 > KW 40 > Datenschützer verabschieden neues Prüfmodell

« Vorige | Nächste »

Datenschützer verabschieden neues Prüfmodell

heise online 01.10.2015 14:13 Uhr – Christiane Schulzki-Haddouti vorlesen

(Bild: BSI)

Die Datenschutz-Aufsichtsbehörden von Bund und Ländern empfehlen, das Standard-Datenschutzmodell anzuwenden. Dieses unterstützt ein strukturiertes Prüfen von IT-Prozessen, was bisher mangels eines eigenen Prüfmodells nicht möglich war.

- 2015-04: Der AK-Technik führt einen **Workshop** zum SDM für alle deutschen Kollegen durch und publiziert einen Tagungsband zum SDM
- 2015-05/09: Erste **SDM-Schulungen** werden an der Datenschutzakademie in Leck/SH durchgeführt.
- 2015-10: Die DSB-Konfererenz nimmt das **SDM-Handbuch** (V0.9) an, das Modell wird auf den Webseiten der deutschen Datenschutzaufsichtsbehörden publiziert und zur Anwendung empfohlen.

Quellen zum SDM

DSB-Konferenz 2010: Modernisierung des Datenschutzrechts
https://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.pdf?__blob=publicationFile

DSB-Konferenz 2015: SDM-Handbuch, V0.9a
https://www.datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf

Arbeitskreis-Technik 2015: Tagungsband "Das Standard-Datenschutzmodell - Der Weg vom Recht zur Technik"
https://www.datenschutz-mv.de/datenschutz/sdm/Tagungsband.pdf

Vielen Dank für Ihre Aufmerksamkeit!

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

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