# Grundlegende Anforderungen des Datenschutzes - Umsetzung mit dem Standard-Datenschutzmodell

**Martin Rost**

## DINI eV: „Datenschutz und Forschungsinformationssysteme“

**02. Februar 2015, Göttingen**

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

# Gliederung

- Was meint „Datenschutz“?
- Der Regelungskern des Datenschutzrechts
- Zur Situation des Datenschutzes an den Hochschulen
- Schutzziele des Datenschutzes und das Standard-Datenschutzmodell (SDM)
- Datenschutzmodellierung eines Forschungsprojekts

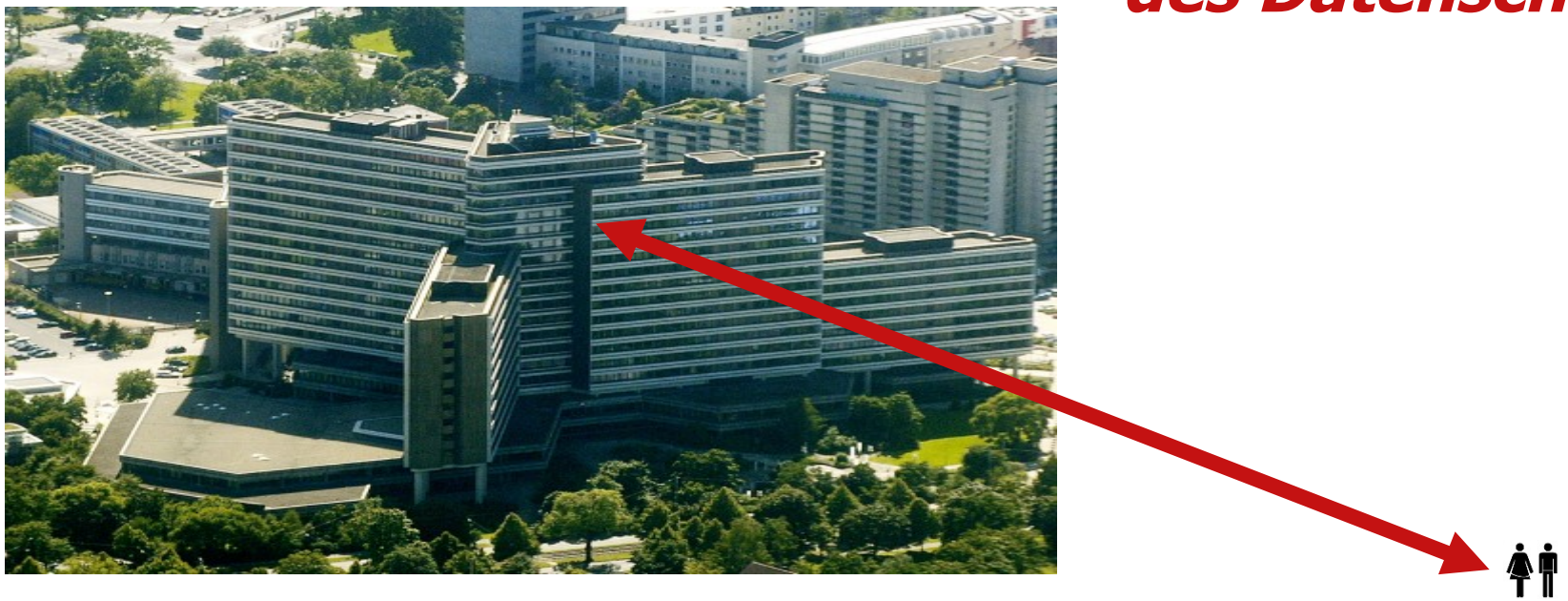
... ist nicht mit *Datenschutzrecht* gleichzusetzen.
**=> juristischer Kurzschluss**

… ist nicht mit *IT-Sicherheit* gleichzusetzen.
**=> technizistischer Kurzschluss**

… ist nicht mit einem *privaten Bedürfnis nach Privatheit* gleichzusetzen.
**=> psychologistischer Kurzschluss**

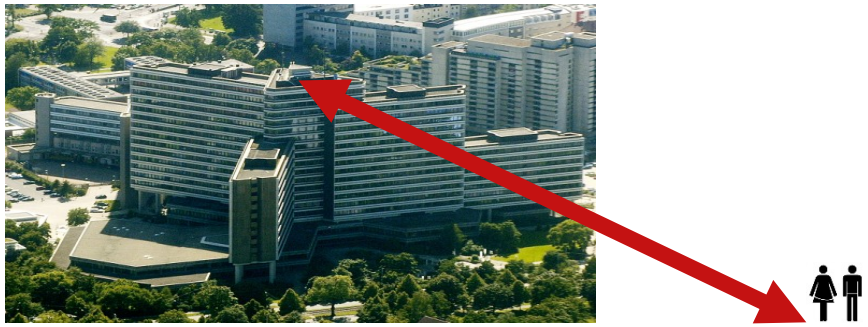
# Was ist „Datenschutz“?

# Objektbereich des Datenschutzes



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

# Objektbereich des Datenschutzes



**Strukturelle Machtasymmetrien werden im Rechtsstaat unter Bedingungen gestellt...**

- durch **gesetzliche Vorgaben** (Grundrechte, Spezialgesetze, Datenschutzgesetze)
  Grundrechte sind Abwehrrechte von Bürgern gegenüber Organisationen, insbesondere dem Staat.
- und **Beratungs-, Prüf- und Sanktionsinstanzen**.

# Anforderung
# DER datenschutzrechtliche Regelungsgrundsatz

**Es dürfen keine personenbezogene Daten verarbeitet werden PUNKT**

Eine Ausnahme von diesem Grundsatz ist zulässig, wenn ein Gesetz die Verarbeitung regelt oder eine Einwilligung durch den Betroffenen vorliegt.

**„Das Verbot mit Erlaubnisvorbehalt"**

**(§ 4 Abs. (1), BDSG )**

# Grundrecht Datenschutz

## 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.

# Datenschutz
## Aktuell geltende Normen

**Bundesdatenschutzgesetz** (BDSG) erstreckt sich auf Privatpersonen, Privatwirtschaft und Bundesbehörden

**Landesdatenschutzgesetze** erstrecken sich auf öffentliche Verwaltung in Land und Kommunen

- speziell in SH: **DS-Verordnung**

**EU: Europäische Grundrechte-Charta**

- **Datenschutz-Richtlinie**
  Wirkung über Import in deutsche Gesetze
- Entwurf: **EU-DS-Verordnung**, die BDSG/LDSGe ersetzen wird!

**Spezialgesetze (haben Vorrang)**:

- Telemedien-Gesetz, T-Kommunik-Gesetz,
- SGB, AO, LandesMeldeGes, LVerwGesetz/ PolizeiGes, PassGes, PersonalausweisGes, AufenthaltsGes., ...

- Rechtmäßigkeit der Datenverarbeitung
  - Gesetzliche Rechtsgrundlagen
  - Einwilligung
- Grundsatz der Zweckbindung
- Grundsatz der Erforderlichkeit
- Grundsatz der Datenvermeidung und Datensparsamkeit
- Grundsatz der Transparenz
- Grundsatz der klaren Verantwortlichkeit
- Grundsatz der Kontrolle
- Grundsatz der Gewährleistung der Betroffenenrechte
  - Verbot der Profilbildung
  - Verbot der Sammlung auf Vorrat
  - Verbot der automatisierten Einzelentscheidung
- Nutzung anonymisierter oder pseudonymisierter Daten

# *Zur Datenschutzsituation an den Hochschulen*

# Allgemeine Datenschutzanforderungen bei Medizin-/Sozialforschung

- Erlaubnis-**Rechtsgrundlage**: Freiheit der Wissenschaft, Forschung und Lehre gemäß Art. 5, Abs. 3 Grundgesetz.
- **Schutzbedarf** von personenbezogenen Forschungsdaten ist generell mit „hoch" anzusetzen.
- Den Befragten (**Einwilligung**) sowie einer Genehmigungsinstanz (bspw. Kultusministerium) ist der **Zweck** darzulegen, es ist transparent zu machen, was und wie protokolliert wird (bspw. Zeitdauer, Suchwege, IP-Adresse), und wie **Protokolle kontrolliert** werden.
- Erstellung eines **Verfahrensverzeichnisses** sowie IT- und Sicherheitskonzept
- „**Datenverarbeitung im Auftrag**" ist zu regeln, wenn RZ, externes RZ oder Umfrageinstitut/Interviewer genutzt werden.
- Nachzuweisendes **Löschen der Daten** nach Durchführung der Untersuchung (oder Übermittlung ans Archiv ist zu regeln).

# Spezifische Anforderungen bei Medizin-/SozialForschung

- Eine Erhebung personenbezogener Daten muss stets an ein bestimmtes **Forschungsprojekt** geknüpft sein.
- Ein Forschungsprojekt muss für so **gewichtig eingeschätzt** werde, dass es die Gewinnung personenbezogener Daten, und damit ein gewisses Eindringen in die Privatsphäre des Einzelnen, rechtfertigt.
- Die Forscher haben zu überlegen, welches methodische Design zur Überprüfung der Forschungshypothesen am **wenigsten in die Privatsphäre der Zielpersonen** eindringt.
- Klären, ob ein Forschungsprojekt eine eigene empirische Erhebung benötigt, ansonsten ist die **Nutzung von vorhandenen Datenbeständen zu bevorzugen**.

# Befunde ULD(1)

Datenschutzbeauftragte an deutschen Hochschulen…

- Zeitkontingente: 5% bis 50%
- meist Juristen, wenig Technik-know-how
- **Aktivitäten meist einzelfall**- und anlaßgesteuert, keine Strategien eines systematisch angelegten Datenschutzmanagements
    - **Keine Beteiligung bei Planungen** von Forschungsprojekten, bei Verfahrensänderungen in der Verwaltung oder bei Prüfungsordnungen.
    - **Keine Beteiligung bei Sicherheitsvorfällen**, keine Beteiligung bei Störungen, Problemen oder Systemänderungen der Verfahren oder der IT.

# Befunde ULD(2)

- Awareness für Anforderungen an Datensicherheit und Datenschutz durch Leitungsebene, jedoch **keine hinreichende Orientierung im Datenschutzrecht**
- Trotz der vergleichsweise reiferen Prozesse der Hochschul-verwaltung: **Mangelnde Dokumentation** (keine aktuellen GV-Pläne noch Dienstanweisungen, Verträge, Systemdoku).
- Hochschul-RZen haben erst vor kurzem begonnen, standardisierte Prozesse für **IT-Service-Strategien** (ITIL oder CoBIT) und Sicherheitsmanagement (IT-Grundschutz oder ISO27001) zu implementieren.
- Institute agieren bei IT-Anforderungen meist „**hemdsärmelig**", (NAS ohne Rechtkontrolle; E-Mailaccounts zu schnell oder gar nicht gelöscht nach Verlassen der Uni)
- Die Systemdadministration agiert in der Regel technisch kompetent, verfügt aber über keine systematische Admin- bzw. spezifische Systembetreuungs-Ausbildungen (**Fortbildungsdefizit**).

# Typische Fehler (3)

- Unklarheiten zu **Verantwortlichkeit** (Verfahren, Technik).
- Keine Regelung und Kontrolle der **Systemadministratoren** auf den Computern.
- Die Einrichtung von **Zugriffsrechten** (wer hat wann wem welche Rechte eingeräumt?) nicht geregelt/prüfbar.
- Die Umsetzung von **Prüfungsordnungen in EDV ohne QM** bzw. ohne geregelte Test & Freigabe-Prozesse.
- **Nicht-Befugte haben Zugriff auf Noten** von Studierenden sowie auf Passworte bei externen Zugängen.
- Es werden zur Auswertung von Untersuchungsdaten auch **private PCs** eingesetzt, die keiner Kontrolle oder Kontrollierbarkeit seitens der Institutsleitung unterliegen.

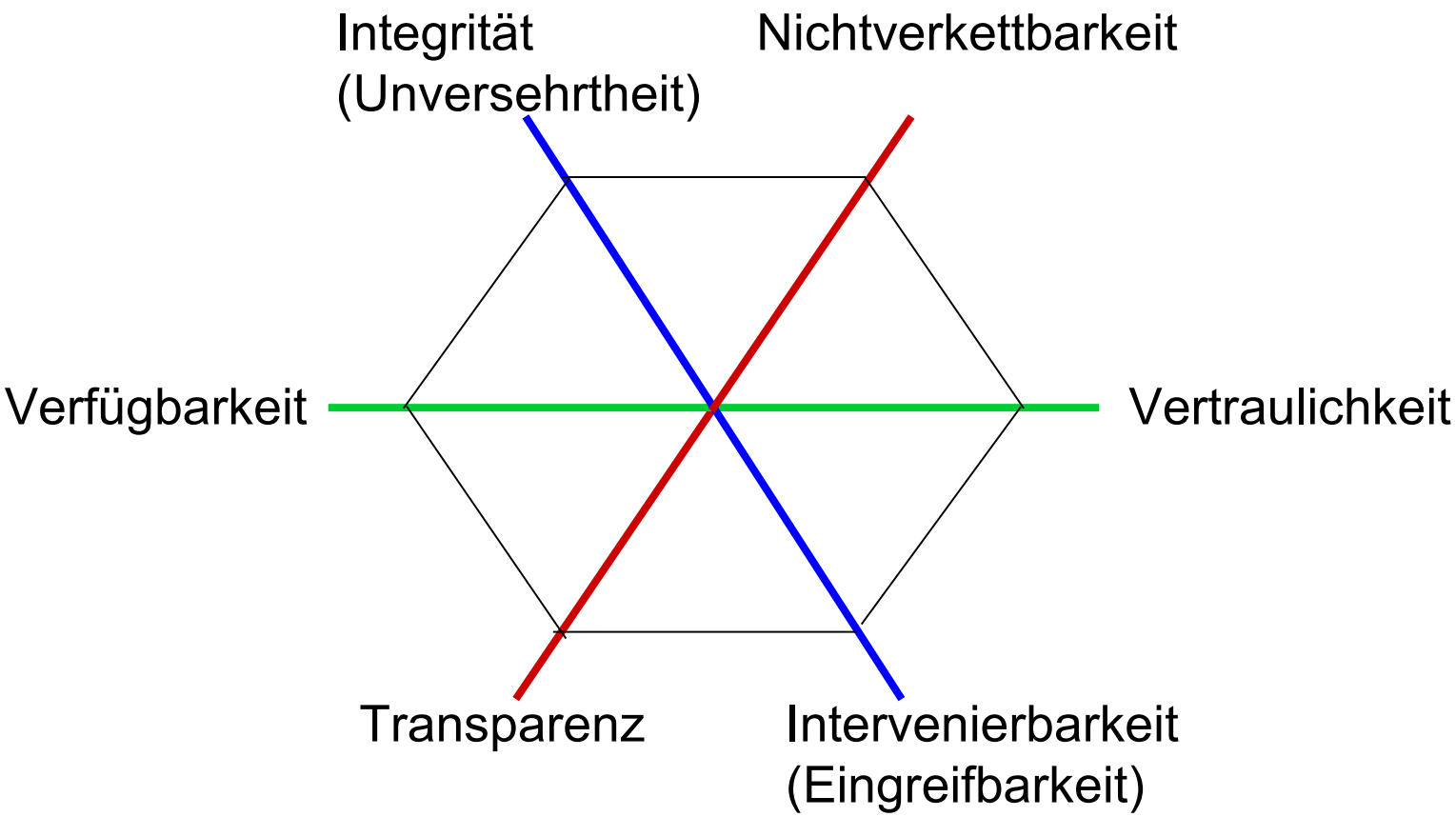
# Schutzziele

# Schutzziele § 5 LDSG-SH

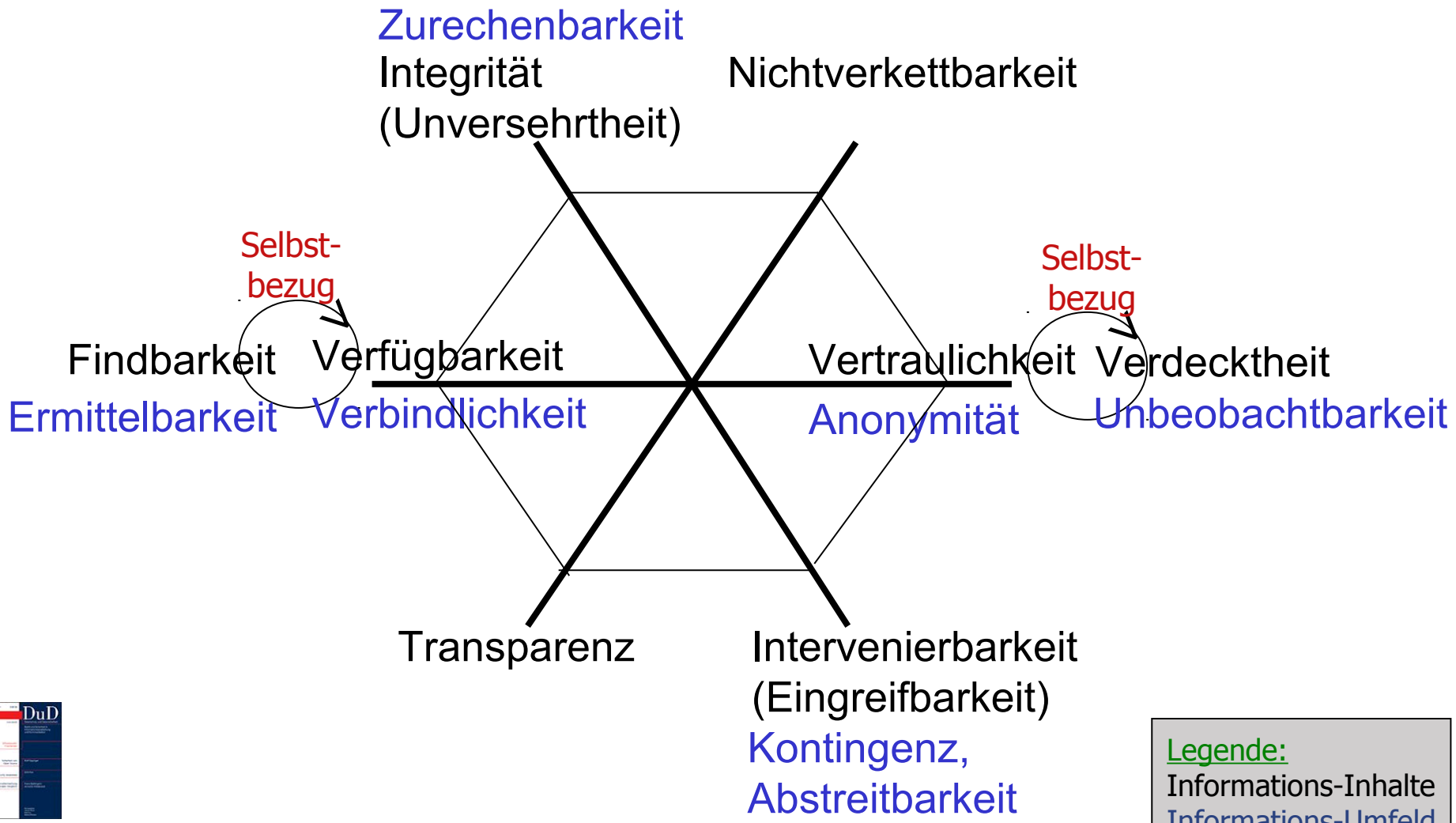
(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz im Sinne von § 3 Abs. 3 ist durch technische und organisatorische Maßnahmen sicherzustellen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. Sie müssen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

# Die elementaren Schutzziele und deren Systematik



# Schutzziele Systematik, vollständig

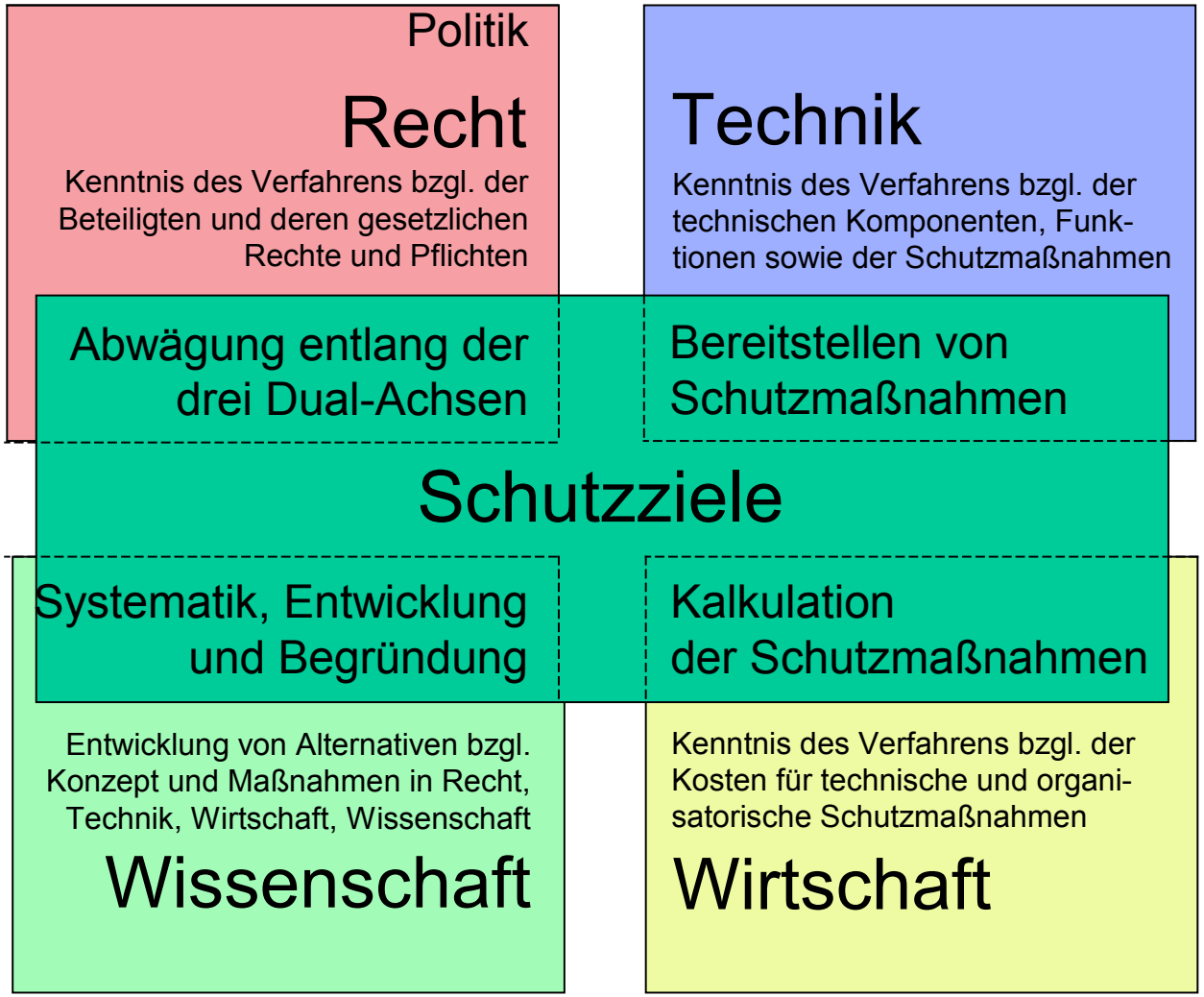





Rost, Martin / Pfitzmann, Andreas, 2009:
**Datenschutz-Schutzziele - revisited**;
in: DuD - Datenschutz und Datensicherheit,
33. Jahrgang, Heft 6, Juli 2009: 353-358

Legende:
Informations-Inhalte
Informations-Umfeld

# Schutzziele als „Universalvermittler"




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

# Zum Verhältnis von Datenschutz und Datensicherheit

Die IT-Sicherheit unterstellt:

**Jede Person kann ein Angreifer sein!**
Die Person muss nachweisen, dass sie kein Angreifer auf die Geschäftsprozesse ist und dass sie ggfs. mit einem Zugriff auf ihre Person rechnen muss.

Der Datenschutz unterstellt:

**Jede Organisation IST ein Angreifer!**
Ein Organisation muss prüffähig nachweisen, dass sie kein Angreifer ist, sich an die Gesetze hält und ihre Verfahren und Prozesse vertrauenswürdig, d.h. ordnungsgemäß beherrscht.

# Das Standard-Datenschutzmodell (SDM)

# Schutzziele gemäß § 5 LDSG-SH

- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Transparenz
- Nicht-Verkettbarkeit
- Intervenierbarkeit

# Schutzmaßnahmen

Sicherstellung von **Verfügbarkeit**
- Daten/Prozesse: Redundanz, Schutz, Reparaturstrategien

Sicherstellung von **Integrität**
- Daten / Systeme: Hash-Wert-Vergleiche
- Prozesse: Festlegen von Min./Max.-Referenzen, Steuerung der Regulation

Sicherstellung von **Vertraulichkeit**
- Daten: Verschlüsselung
- Systeme / Prozesse: Rollentrennungen, Abschottung, Containern

Sicherstellen von **Nichtverkettbarkeit** durch Zweckbestimmung/-bindung
- Daten: Pseudonymität, Anonymität (anonyme Credential)
- Prozesse: Identitymanagement, Anonymitätsinfrastruktur, Audit

Sicherstellen von **Transparenz** durch Prüffähigkeit
- Daten / Systeme / Prozesse: Protokollierung, Dokumentation von Verfahren

Sicherstellen von **Intervenierbarkeit** durch Ankerpunkte
- Daten: Zugriff auf Betroffenen-Daten durch den Betroffenen
- Prozesse: SPOC für Änderungen, Korrekturen, Löschen, Aus-Schalter, Changemanagement,

# Verfahrenskomponenten

## Schutz-ziele

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

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

Thomas Probst: **Generische Schutzmaßnahmen für Datenschutz-Schutzziele**; in: DuD 2012/06.: 439-444

# Verfahrens-komponenten

Ein Verfahren besteht aus drei zu betrachtenden Komponenten:

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

# Schutzbedarfe für Betroffene

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.)

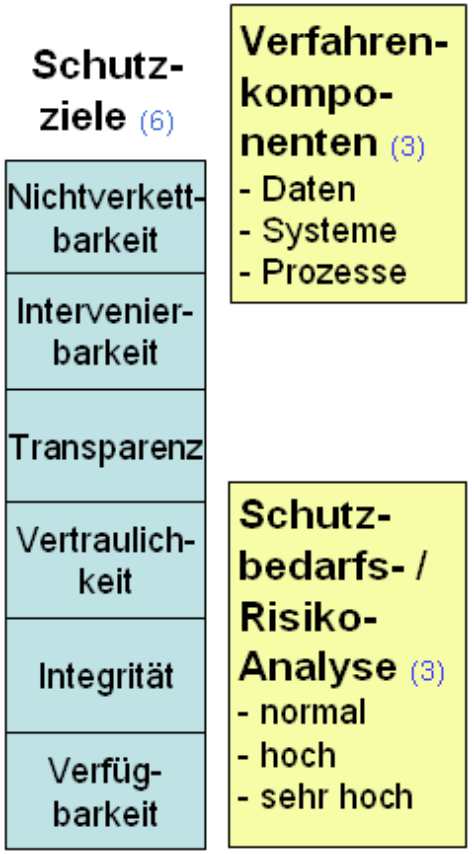
# Komponenten des Standard-Datenschutzmodells

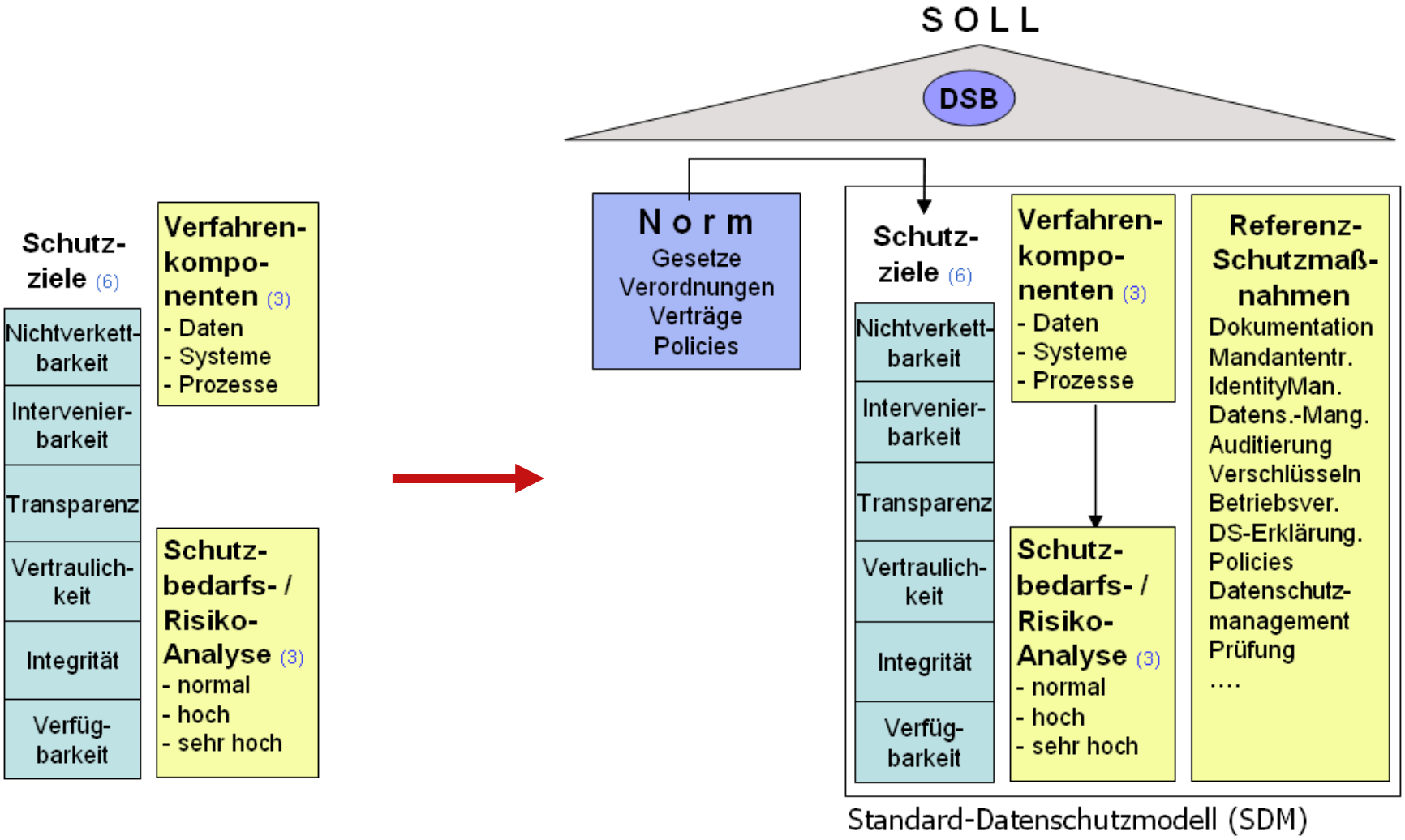
3 Schutzbedarfsabstufungen, aus der Betroffenenperspektive!

6 Schutzziele, hinterlegt mit Maßnahmen-Katalog!

3 Verfahrenskomponenten!

Dies entspricht einem Referenzmodell für 6x3x3 (54) spezifische Datenschutzmaß-nahmen, gegen das sich jedes personenbezogene Verfahren standardisiert prüfen lässt!



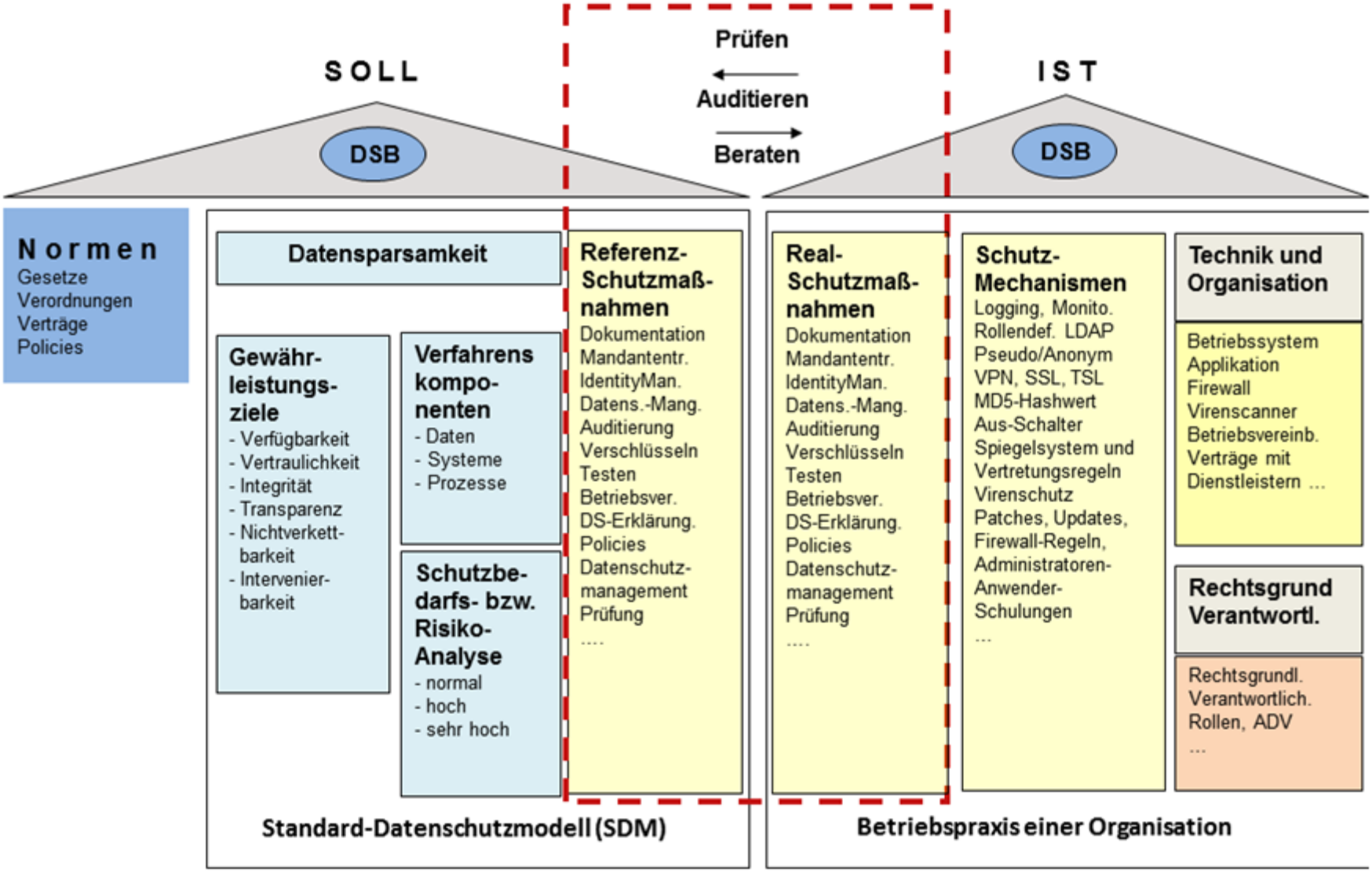



Standard-Datenschutzmodell (SDM)

# Aktueller Status des SDM

**Beschluss der 88. Datenschutzkonferenz Oktober (2014):**

- Der Entwurf des Handbuchs zum Standard-Datenschutzmodell (Version 0.8) wurde zustimmend zur Kenntnis genommen.
- Auftrag: Ein **Katalog mit Referenzschutzmaßnahmen ist bis Oktober 2015** zu entwickeln.
- Übersetzung des Handbuchs ins Englische und Vorlage bei der Art. 29-Gruppe.
- Status: Bleibt internes Arbeitspapier der DSK.


SOLL
Prüfen
Auditieren
Beraten
IST
DSB
DSB
Normen
Gesetze
Verordnungen
Verträge
Policies
Datensparsamkeit
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
....
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.
Rechtsgrundl.
Verantwortlich.
Rollen, ADV
...
Standard-Datenschutzmodell (SDM)
Betriebspraxis einer Organisation

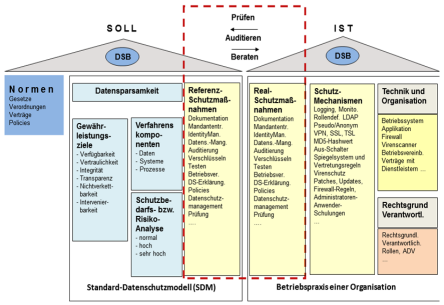
# Datenschutz-würfel für Forschungsprojekte

Umsetzung der Schutzmaßnahmen

1. Gesetzliche Anforderungen
2. Rechtliche Abwägung der Schutzziele
3. Schutzmaßnahmenkataloge

## Datenschutz-Schutzziele

- Intervenierbarkeit
- Nicht-Verkettbarkeit
- Transparenz
- Vertraulichkeit
- Integrität
- Verfügbarkeit




**Weitere externe Akteure**
- Versicherungen
- Sicherheitsbehörden
- Aufsichtsbehörden
- Verwaltungen
- Access-, Content-, IT-Provider
- selbstorganisierte Netzwerke

Rechtsbeziehungen

Prozesseigentümer = Verantwortlichkeiten

**Prozesse**

Auftrags-DV/ RZ, „DL des DL“

Operative Unterstützung durch: Standards, Zertifizierungen

Organisation/ Dienstleister

Operative Unterstützung durch: Datenschutz-Managementsystem

Betroffener

**Daten**

Technische Systeme

Schutzbedarfs-feststellung

| Interventionsdaten | Vitaldaten | Verhaltensdaten | IT-Infrastrukturdaten | Umgebungsdaten | Aggregierte Daten |
|---|---|---|---|---|---|
| - Fernmedikamentgabe<br>- Fernjustage<br>- Raumzutritt<br>- … | - Blutdruck<br>- Blutzucker<br>- Temperatur<br>- Stuhlgang<br>- EKG<br>- … | - Bewegung<br>- Liegedruck<br>- Türöffnungen<br>- Video-/Audioüberwachung<br>- Nutzung von Herd/WC/TV/PC<br>- … | - Still-Alive-Pings<br>- Protokoll/Logs<br>- Sensor-Rohdaten<br>- … | - Temperatur<br>- Licht<br>- Lautstärke<br>- … | - Abrechnungsdaten über Kommunikation<br>- Energieverbrauch<br>- Alarmtrigger<br>- … |

# *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
https://www.datenschutzzentrum.de/