# Gute Methodik und zutreffende Modellierung von Datenschutz

Martin Rost

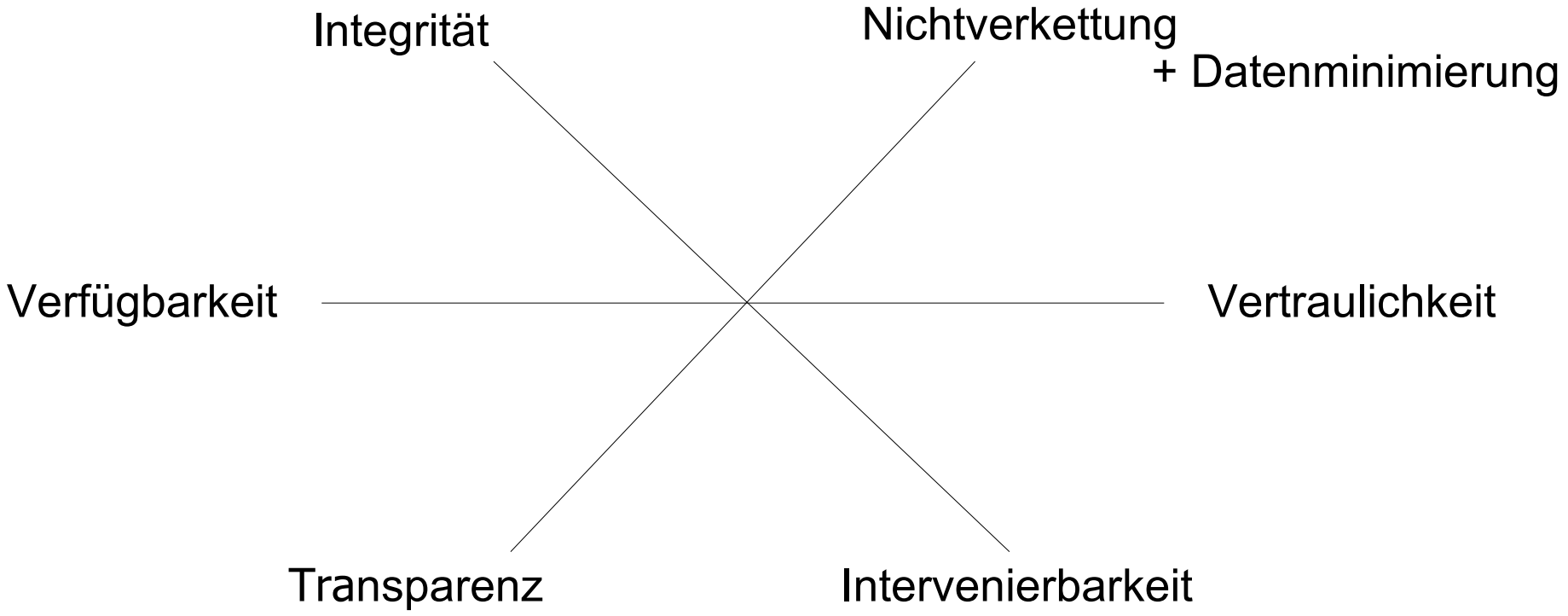
22.03.2018, Berlin


# Agenda

1. Was meint „Datenschutz“?
2. Objektbereich des Datenschutzes
3. Datenschutz-Risiken
4. Komponenten des Standard-Datenschutzmodells (SDM)
5. Beispiele: Protokollierung nach SDM / Datenschutz-Folgenabschätzung mit SDM”
6. Zum nicht unproblematischen Verhältnis von Informationssicherheit und operativem Datenschutz
7. Referenzen und Kontakt

# Zusammenfassung Modellierung Datenschutz

- Schutzobjekt sind natürliche Personen, nicht Organisationen
- Risiken entstehen primär durch Verarbeitung, nicht durch IT-Sicherheit
- Es sind 6+1 Schutzziele anzustreben, nicht 3, umzusetzen mit spezifischen Maßnahmen



# *Was meint „Datenschutz“?*

- **Datenschutz ist nicht mit Datenschutzrecht gleichzusetzen!**

  Denn das Datenschutzrecht reagiert auf einen strukturellen Konflikt. Nur: Worin genau besteht dieser strukturelle Konflikt?

- **Datenschutz ist nicht mit der IT-Sicherheit gleichzusetzen!**

  Ein technisch sicheres System kann vollkommen unrechtmäßig betrieben werden, es ist deshalb mit Konflikten zw. Datenschutz und IT-Sicherheit zu rechnen, grundrechtlich führt Datenschutz. Datenschutz gilt Betroffenen, nicht Organisationen.

- **Der Grund für Datenschutz ergibt sich nicht aus einem individuellen Bedürfnis nach Privatheit.**

  Das Konzept „informationelle Selbstbestimmung“ ist eine funktionale Voraussetzung moderner Gesellschaften.

# *Der Objektbereich des Datenschutzes*

Datenschutz beobachtet, beurteilt und gestaltet die asymmetrischen Machtbeziehungen zwischen Organisationen und Personen... aus der Perspektive des Risikonehmers “Person”.

# *Verhältnis IT-Sicherheit – Datenschutz*

- IT-Sicherheit unterstellt methodisch:

  **Jede Person kann ein Angreifer sein!**

  - Risikogeber: Person,
  - Risikonehmer: Organisation.

- Datenschutz unterstellt methodisch:

  **Jede Organisation ist ein Angreifer!**

  - Risikogeber: Organisation, sie erzeugt durch Verarbeitung von Daten Risiken für Personen.
  - Risikonehmer: Person.

Für Kryptologen: Insbesondere Bob ist Angreifer!

**DER datenschutzrechtliche Grundsatz des kontinentaleuropäischen Datenschutzrechts lautet:**

Organisationen dürfen keine personen-bezogenen Daten verarbeiten PUNKT

# *Die zentralen Regelungsstrategie der DSGVO*

## „Verbot mit Erlaubnisvorbehalt“

### Artikel 6 DSGVO

Organisationen dürfen keine personenbezogenen Daten erheben, verarbeiten und nutzen, es sei denn, dass

- ein **Gesetz** die Verarbeitung regelt, was insbesondere für den öffentlichen Bereich gilt oder wenn
- eine **Einwilligung** vorliegt, was für den privaten Bereich zentral ist und insbesondere an die Bestimmung eines legitimen Zwecks, der Freiwilligkeit der Erteilung und an umfassende Auskünfte an Empfänger und deren verarbeitungsmotive geknüpft ist.

# *Zentrale Vorgaben für das Datenschutzrecht durch EU-Charta (2010)*

## Grundgesetz

*Artikel 1*

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

*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.

## EU-Grundrechte-Charta

*Artikel 1*

Die Würde des Menschen ist unantastbar. Sie ist zu achten und zu schützen.

*Artikel 8*

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Grundrecht auf Datenschutz

Verbot mit Erlaubnis-vorbehalt

Datenschutz-kontrolle

# Agenda

1. Was meint „Datenschutz“?

## 2. Objektbereich des Datenschutzes

3. Datenschutz-Risiken
4. Komponenten des Standard-Datenschutzmodells (SDM)
5. Beispiele: Protokollierung nach SDM / Datenschutz-Folgenabschätzung mit SDM”
6. Zum nicht unproblematischen Verhältnis von Informationssicherheit und operativem Datenschutz
7. Referenzen und Kontakt

# *Modellierungsobjekt im Datenschutz ist eine "Verarbeitung" (durch eine Organisation)*

*Art. 4, Abs. 2, DSGVO:* "Im Sinne dieser Verordnung bezeichnet der Ausdruck: „**Verarbeitung**" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie

- das Erheben,
- das Erfassen,
- die Organisation,
- das Ordnen,
- die Speicherung,
- die Anpassung oder Veränderung,
- das Auslesen,
- das Abfragen,
- die Verwendung,
- die Offenlegung durch Übermittlung,
- Verbreitung oder eine andere Form der Bereitstellung,
- den Abgleich oder die Verknüpfung,
- die Einschränkung,
- das Löschen oder die Vernichtung; (….)"

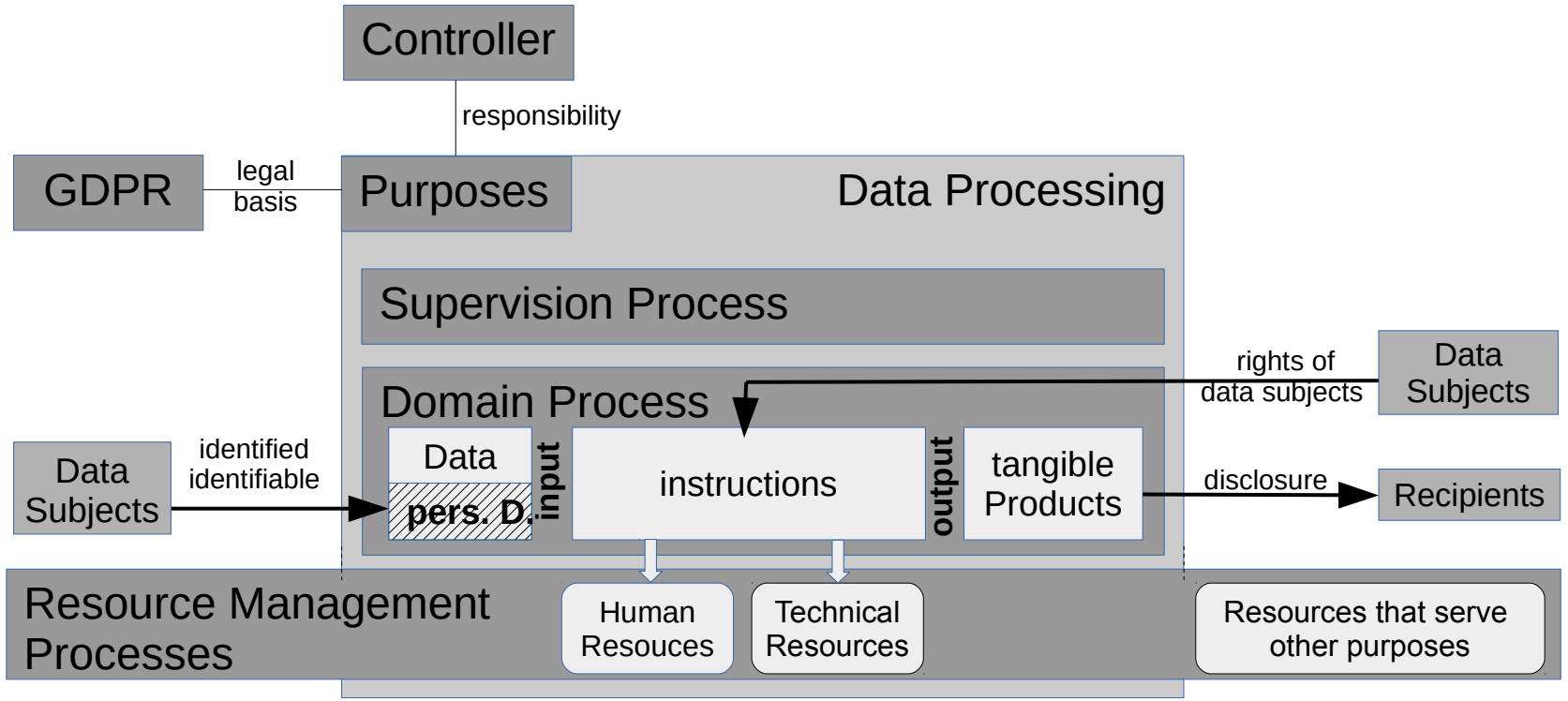
# *Verarbeitung*

Eine Verarbeitung...

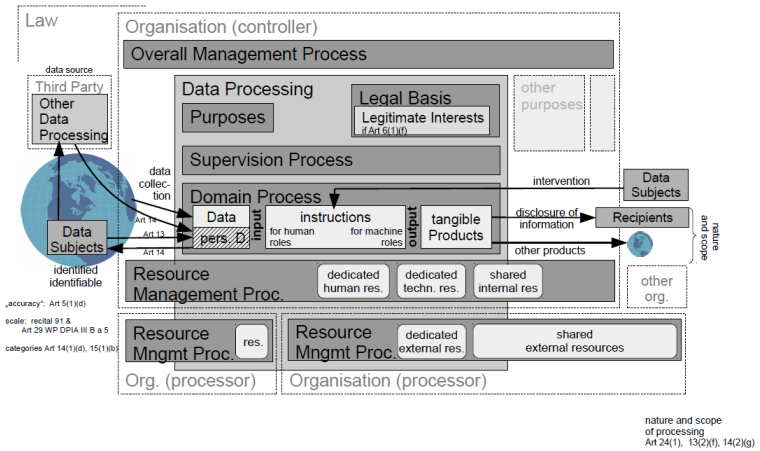
- ist eine Aktivität einer **Organisation**;
- hat einen **Verantwortlichen**;
- wird bestimmt durch einen (oder mehrere kompatible) **Zweck;**
  - Zwecksetzung
  - Zweckbeschreibung oder Zweckdefinition
  - Zwecktrennung
  - Zweckbindung (horizontal, vertikal)
- ist in der Regel als Sachbearbeitung mit den Komponenten **Daten, IT-Systemen und Prozessen** implementiert.

# Modellierung

## von “Verarbeitung” (“data processing”, ehemals: “Verfahren”)?

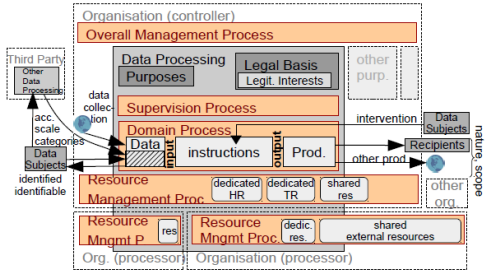



Resources can be provided by the Controller and/or Processors




Data Processing involves several **Processes**

- **Overall Management Process** of the Organization.
- A **Domain Process** that implements the actual purposes.
- One to several **Resource Management Processes** that provide the necessary Resources to the Domain Process.
- A **Supervision Process** that manages the Domain Process and its execution on assigned Resources.




Grafik: Dr. Bud P. Bruegger (ULD), 2018-0310

# Agenda

1. Was meint „Datenschutz“?
2. Objektbereich des Datenschutzes

## 3. Datenschutz-Risiken

4. Komponenten des Standard-Datenschutzmodells (SDM)
5. Beispiele: Protokollierung nach SDM / Datenschutz-Folgenabschätzung mit SDM”
6. Zum nicht unproblematischen Verhältnis von Informationssicherheit und operativem Datenschutz
7. Referenzen und Kontakt

# *Was ist ein Datenschutz-Risiko?*

Das spezifische Datenschutz-Risiko besteht darin, dass die **Anforderungen der DSGVO** durch die Verarbeitungstätigkeiten von Organisationen gegenüber Personen nicht in dem Maße umgesetzt werden, dass der Eingriff in die Rechte und Freiheiten der Personen auf das Mindestmaß reduziert ist.

# Datenschutz-Risiken durch Negieren der Anfoderungen nach Art. 5 DSGVO

Art. 5 Abs. 1 „Personenbezogene Daten müssen“

(a) „... in einer für die Person nachvollziehbaren Weise verarbeitet werden ... (**Transparenz**).“
(b) „... für festgelegte eindeutige und legitime Zwecke erhoben werden ... (**Zweckbindung**).“
(c) „... auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**Datenminimierung**).“
(d) „... damit personenbezogene Daten, die im Hinblick auf die Zwecke der Verarbeitung unrichtig sind, ... **unverzüglich gelöscht oder berichtigt** werden.“
(f) „... **Schutz vor Verlust** ... **Integrität und Vertraulichkeit**“.

**Risiken durch Negation der Anforderungen:**

***Intransparenz***

***Beliebige Verkettung***

***Beliebige Datenfülle***

***Keine Intervenierbarkeit***

***Mangel an Verfügbarkeit***
***Mangel an Integrität***
***Mangel an Vertraulichkeit***

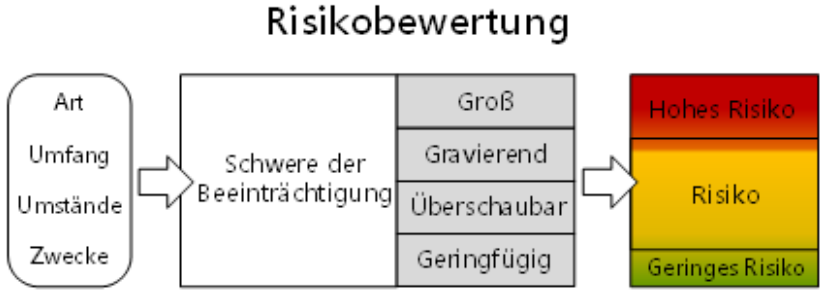
# *Operativer Datenschutz*

- Das spezifische operative Datenschutz-Risiko besteht insofern darin, dass die **Intensität eines Grundrechtseingriffs durch die Organisation nicht auf ein ausreicheides Maß verringert wird.** Dieses Risiko besteht auch dann weiter fort, wenn ein Verfahren vollkommen rechtskonform und mit allen Maßnahmen der Informationssicherheit abgesichert betrieben wird.
- Das spezifische Risiko der Informations- oder **IT-Sicherheit besteht darin, dass Unbefugte auf personenbezogene Daten** zugreifen können.

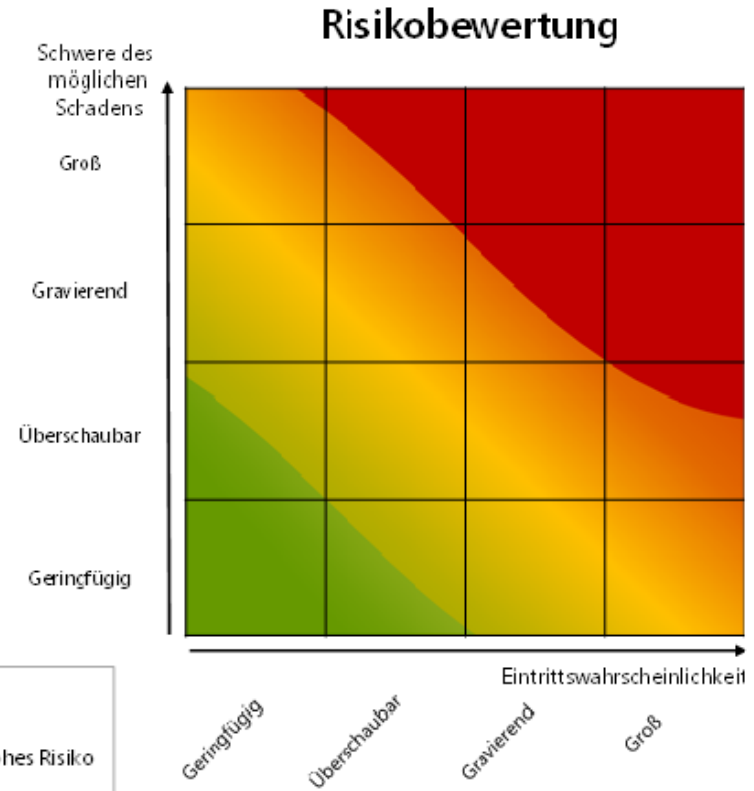
# Risiko

## Grundrechtseingriff und Schäden gem. Art. 24 DSGVO

**1.** Eine **Beeinträchtigung** der Rechte und Freiheiten der Betroffenen entsteht, **wenn der Eingriff durch die personenbezogene Verarbeitung einer Organisation nicht auf ein ausreichendes Maß verringert wird.** Die Beeinträchtigung besteht fort auch bei einem rechtskonformen und sicheren IT-Betrieb.




**2. Schäden** durch unzulängliche Verfahrensgestaltung und **unzulängliche Absicherungen der IT** nach der Formel: *Risiko = Eintrittswahrscheinlichkeit x Schwere des Schadens*




Aus: Entwurf Kurzpapier Nr. 10 „Risiko für die Rechte und Freiheiten natürlicher Personen“ (Entwurf: 19.12.2017)

# *Risiken im Datenschutz, aus Betroffenenperspektive*

**Risiken** bzgl. Rechte und Freiheiten von Personen entstehen, wenn Organisationen Verfahren betreiben, für die

1. die **Legitimität** nicht festgestellt ist
2. die Rechtsgrundlage fehlt oder nicht ausreicht.
3. eine **zu geringe Eingriffsintensität** ausgewiesen ist.
4. die **Schutzmaßnahmen des operativen Datenschutzes** zur Minimierung der Eingriffsintensität nicht wirksam implementiert oder konfiguriert sind.
5. Daten **zwecküberdehnend** verarbeitet werden.
6. die **Maßnahmen der IT-Sicherheit** nicht hinreichend implementiert oder konfiguriert sind → **Schäden**
7. die **Maßnahmen der IT-Sicherheit nicht datenschutz-gerecht** implementiert oder konfiguriert sind.
8. **keine Datenschutzkontrolle,** weder organisationsintern oder extern durch DS-Aufsicht, vorgesehen ist.

Im Scope der DSGVO

## EG 75 DSGVO zu Schäden:

- Diskriminierung,
- Identitätsdiebstahl oder -betrug,
- finanzieller Verlust,
- Rufschädigung,
- wirtschaftliche oder gesellschaftliche Nachteile,
- Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen.

# Agenda

1. Was meint „Datenschutz“?
2. Objektbereich des Datenschutzes
3. Datenschutz-Risiken

## 4. Komponenten des Standard-Datenschutzmodells (SDM)

5. Beispiele: Protokollierung nach SDM / Datenschutz Folgenabschätzung mit SDM”
6. Zum nicht unproblematischen Verhältnis von Informationssicherheit und operativem Datenschutz
7. Referenzen und Kontakt

# Schnellübersicht

## Standard-Datenschutzmodell aktueller Stand (2017/04)

**Datenschutzkonferenz gibt sich Grundlagen und kritisiert Innenminister**

heise online 11.11.2016 12:40 Uhr – Christiane Schulzki-Haddouti vorlesen

Auch de Maizières Entwurf eines Videoüberwachungsverbesserungsgesetzes bekam sein Fett ab.

**Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat ihre Kontroll- und Beratungspraxis auf eine systematische und konsistente Grundlage gestellt. Auch hatten sie vielfach Kritik an Innenminister parat.**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist am gestrigen Donnerstag mit wegweisenden Entschließungen zu Ende gegangen. Mit der eigenen Prüfsystematik sind die Aufsichtsbehörden einen wesentlichen Schritt vorangekommen: So wollen sie das Handbuch zum Standard-Datenschutzmodell (SDM) in der aktuellen Version als Erprobungsfassung herannnehmen.

*Heise-Online: 11. November 2016*

- Die DSB-Konferenz hat 2016/11 die **SDM-Methodik** im SDM-Handbuch (52 Seiten), Version 1.0 angenommen, Modell ist auf den Webseiten der deutschen Datenschutzaufsichtsbehörden publiziert. V1.1 steht aktuell zur Abstimmung
- **Normative Verankerung in der DSGVO,** Englischübersetzung liegt vor.
- Methodische **Anlehnung an Grundschutz**, Übersicht zum SDM in CON2 ersetzt alten Datenschutzbaustein M1.5, die GS-Bausteine zum Datenschutz sind im SDM aufgegangen.
- Kap. 7 des Handbuchs listet generische **Maßnahmen** auf, der konkretisierende Maßnahmenkatalog soll in Einzelbausteinen durch AK-Technik veröffentlicht werden, wurde bislang mangels deutschlandweiten Konsens zurückgehalten, **aktuell: Publikationsabsicht eines eigenen Bausteinekatalogs durch SN, MV, HS, SH, EKD**
- Kernteam umfasst ca. 8 Personen aus verschiedenen Aufsichtsbehörden als Unterarbeitsgruppe (**UAGSDM**) des Arbeitskreis-Technik der DSB-Konferenz.
- **Betriebskonzept**:
  - Erarbeiten von Bausteinen bislang nur durch DS-Aufsichtsbehörden
  - Kontrollierte Fortschreibung von Bausteintexten durch CRs
  - QM durch Review innerhalb UAGSDM und AK-Technik

# IT-Grundschutz und SDM

Bundesamt für Sicherheit in der Informationstechnik

LEICHTE SPRACHE

Themen | Das BSI

## IT-Grundschutz

### CON.2 Datenschutz

Schnell zum Abschnitt



Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_2_Datenschutz.html

### 1.1 Einleitung

Aufgabe des Datenschutzes ist es, Personen davor zu schützen, dass diese durch den Umgang mit personenbezogenen Daten auf der Seite von Institutionen an der Ausübung von Grundrechten beeinträchtigt werden. Die Verfassung der Bundesrepublik Deutschland gewährleistet das Recht der Bürgerinnen und Bürger, grundsätzlich selbst über die Verwendung ihrer personenbezogenen Daten zu bestimmen. Die Datenschutzgesetze des Bundes und der Bundesländer nehmen darauf Bezug, wenn sie den Schutz des Rechts auf informationelle Selbstbestimmung hervorheben. Die EU-Grundrechte-Charta formuliert in Artikel 8 unmittelbar das Recht auf den Schutz personenbezogener Daten (Absatz 1), hebt die Notwendigkeit einer Rechtsgrundlage zur Datenverarbeitung hervor (Absatz 2) und schreibt die Überwachung der Einhaltung von Datenschutzvorschriften durch eine unabhängige Stelle vor (Absatz 3). Die Datenschutz-Grundverordnung [DSGVO] führt diese Anforderungen der Grundrechte-Charta näher aus. Von herausragender Bedeutung ist dabei der Artikel 5 DSGVO, der die Grundsätze versammelt, die teilweise als *Schutzziele* ausgewiesen sind. Das Standard-Datenschutzmodell (SDM) bietet eine Methode, um diese geforderte Umsetzung von Datenschutzvorschriften auf der Grundlage von sieben Schutzzielen bzw. Gewährleistungszielen systematisch überwachen zu können.

„**Das Standard-Datenschutzmodell (SDM)** bietet eine Methode, um diese geforderte Umsetzung von Datenschutzvorschriften auf der Grundlage von sieben Schutzzielen bzw. Gewährleistungzielen systematisch überwachen zu können.“

# CON.2-Datenschutz

## Das Standard-Datenschutzmodell hat daher die folgenden Ansprüche:

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

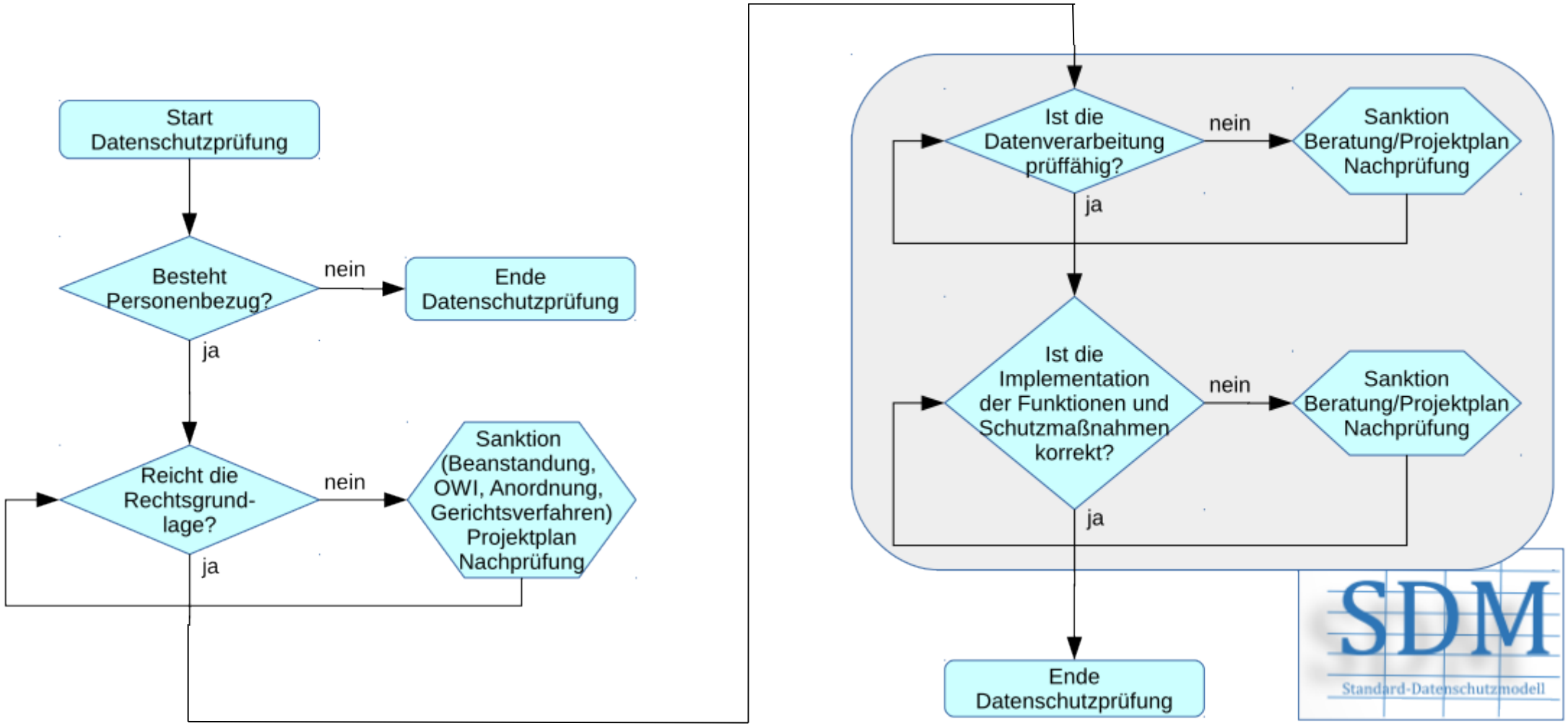
## 2.2 Risiken bei Festlegung eines zu niedrigen Schutzbedarfs

- Die Institution hat den gegenüber der Informationssicherheit erweiterten Schutzzielekatalog des Datenschutzes nicht berücksichtigt.

- Die Institution hat bei der Schutzbedarfsermittlung nicht zwischen den Risiken für die Umsetzung der Grundrechte der Betroffenen und den Risiken für die Institution unterschieden.
- Die Institution hat zwar die beiden Schutzinteressen unterschieden, aber die Funktionen des Verfahrens und der Schutzmaßnahmen zugunsten der Institution bzw. zu Ungunsten betroffener Personen gestaltet.

Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_2_Datenschutz.html

# Standardablauf einer Datenschutzprüfung, Verortung des SDM

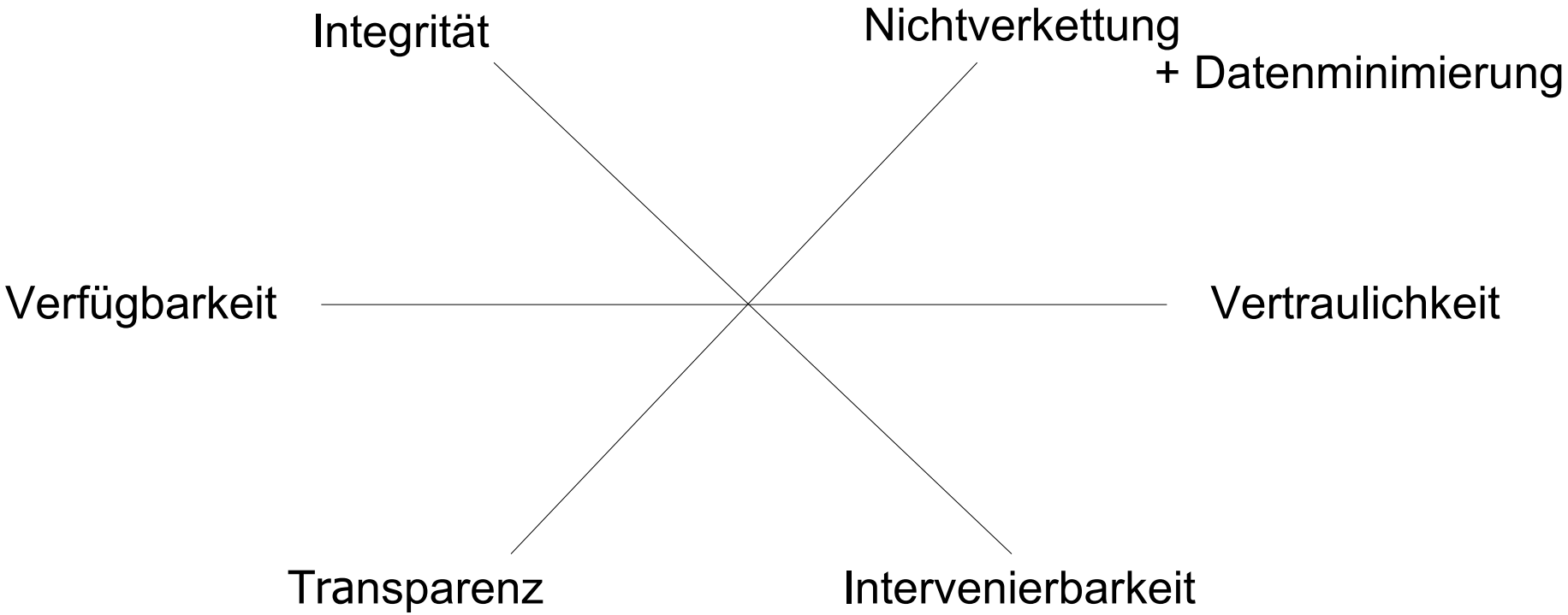



Grafik: M. Rost (ULD)

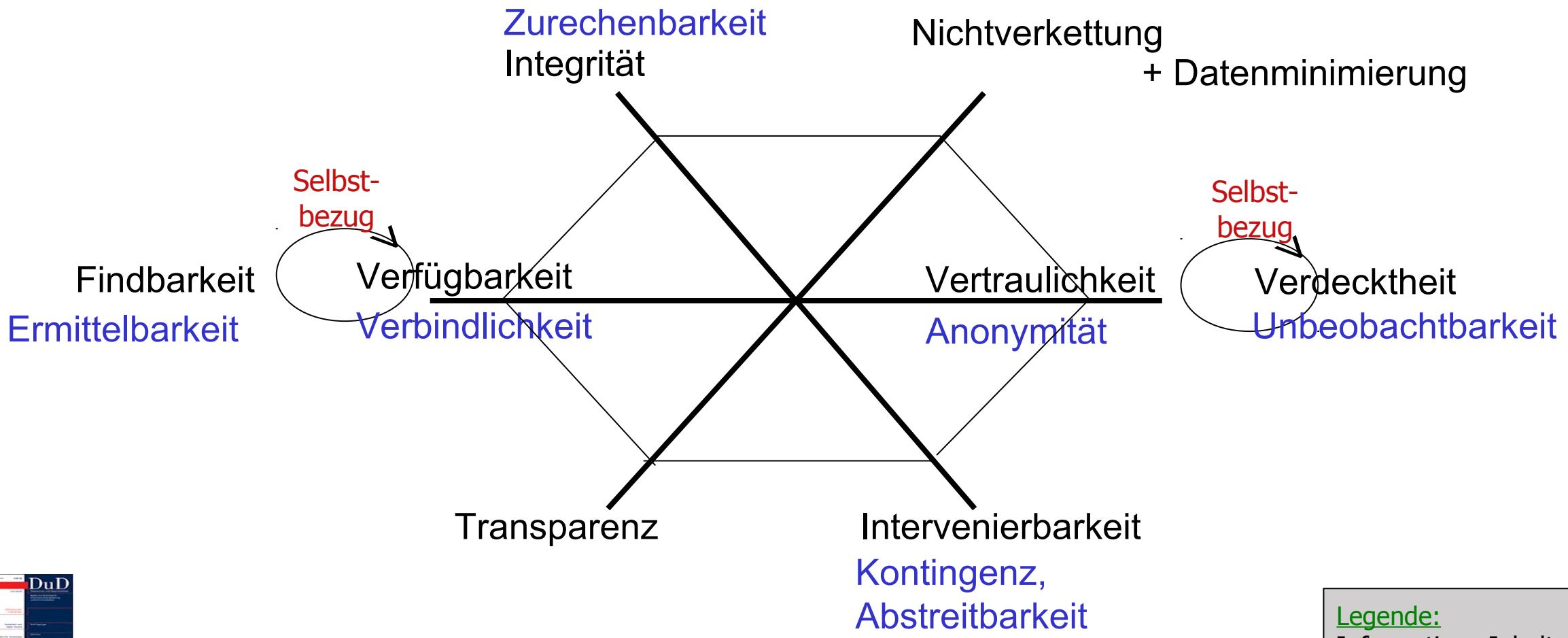
# SDM-Komponente 1:

# “Gewährleistungsziele”

# Systematik der elementaren Gewährleistungsziele des SDM



# *Systematik der Gewährleistungsziele des SDM (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

# *Art. 5 der DSGVO und die Gewährleistungsziele des SDM*

Art. 5 Abs. 1 „Personenbezogene Daten müssen“

(a) „... in einer für die Person nachvollziehbaren Weise verarbeitet werden ... (**Transparenz**).“
(b) „... für festgelegte eindeutige und legitime Zwecke erhoben werden ... (**Zweckbindung**).“
(c) „... auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**Datenminimierung**).“
(d) „... damit personenbezogene Daten, die im Hinblick auf die Zwecke der Verarbeitung unrichtig sind, ... **unverzüglich gelöscht oder berichtigt** werden.“
(f) „... **Schutz vor Verlust** ... **Integrität und Vertraulichkeit**“.

**Transparenz** ✓
**Nichtverkettung** ✓
**Datenminimierung** ✓
**Intervenierbarkeit** ✓
**Verfügbarkeit** ✓
**Integrität** ✓
**Vertraulichkeit** ✓

# Mapping

## Artikel und Erwägungsgründe der DSGVO und Gewährleistungsziele

*Tabelle 3: Zuordnung der Artikel der DS-GVO zu den Gewährleistungszielen.*

| Datenminimierung | Verfügbarkeit | Integrität | Vertraulichkeit | Nichtverkettung | Transparenz | Intervenierbarkeit |
|---|---|---|---|---|---|---|
| 5 I c), 5 I e), 25, 32 | 5 I e), 13, 15, 20, 25, 32 | 5 I f), 25, 32, 33 | 5 I f), 25, 28 III b), 29, 32 | 5 I c), 5 I e), 17, 22, 25, 40 II d) | 5 I a), 13, 14, 15, 19, 25, 30, 32, 33, 40, 42 | 5 I d),5 I f), 13 II c), 14 II d), 15 I e), 16, 17, 18, 20, 21, 25, 32 |

*Tabelle 4: Zuordnung der Erwägungsgründe der DS-GVO zu den Gewährleistungszielen.*

| Datenminimierung | Verfügbarkeit | Integrität | Vertraulichkeit | Nichtverkettung | Transparenz | Intervenierbarkeit |
|---|---|---|---|---|---|---|
| 28, 29, 30, 39, 78, 156 | 49, 78, 83 | 39, 49, 78, 83 | 39, 49, 78, 83 | 31, 32, 33, 39, 50, 53, 71, 78 | 32, 39, 42, 58, 60, 61, 63, 74, 78, 84, 85, 86, 87, 90, 91, 100 | 39, 59, 65, 66, 67, 68, 69, 70, 78 |

aus: SDM-Handbuch, V1.0, S. 24

# *Anker für operativen Datenschutz in der DSGVO*

| | |
|---|---|
| **Art. 5 -** “Grundsätze” (Schutzziele bzw. Gewährleistungsziele) | Fordert generisch, dass Verarbeitungen personen-bezogener Daten **bestimmte Eigenschaften** erfüllen, insbes den Nachweis der Wirksamkeit von Schutzmaßnahmen. |
| **Art. 12 bis 23 -** Umsetzung von Betroffenenrechten | Fordert Einbau **betroffenenspezifischer Funktionen** einer Verarbeitung (Applikation) |
| **Art. 24 -** “Verantwortung” / “Risiko” | Fordert **Nachweisbarkeit** der Umsetzung, gibt Halt für **Skalierbarkeit der Wirksamkeit** von Schutzmaßnahmen |
| **Art. 25 -** “Dataprotection By Design” | Fordert die wirksame Umsetzung genereller Schutz-maßnahmen und betroffenenspezifischer Funktionen während der **Spezifikationsphase.** |
| **Art. 32 -** “Sicherheit”, ISMS, DPMS | Fordert u.a. die permanente **Überwachung** aller Verarbeitungstätigkeiten (DPMS / ISMS) |
| **Art. 35 -** “Datenschutz-Folgenabschätzung” | Fordert **verarbeitungsspezifische Risikoanalyse, Spezifikation** sowie **Implementation** von Funktionen und Schutzmaßnahmen. |

# *Referenzmaßnahmen zur Umsetzung der Gewährleistungsziele*

Sicherstellung von ***Verfügbarkeit***
Redundante Datensätze, IT-Systeme, Prozesse, „schnelle Reparaturzeiten“

Sicherstellung von ***Integrität***
Hash-Wert-Vergleiche, Härten von IT-Systemen, Festlegen von Min./Max.-Referenzen bei Prozessen, Steuerung der Regulation von Prozessen

Sicherstellung von ***Vertraulichkeit***
Verschlüsselung, Rollen- und Berechtigungskonzepte

Sicherstellung von ***Transparenz***
Prüffähigkeit durch Spezifikation, Protokollierung, Dokumentation, Tests und Freigaben

Sicherstellung von ***Nichtverkettbarkeit*** durch Zweckbestimmung/-bindung, Pseudonymität, Anonymität; Trennung und Isolierung von Datenbeständen, IT-Systemen, Prozessabläufen, Rollen- und Berechtigungskonzepte

Sicherstellung von ***Intervenierbarkeit***
SPOC für Änderungen, Korrekturen, Löschen, Aus-Schalter, standardisierte Changemanagementprozesse in Organisationen

# SDM-Komponente 2:

# “Schutzbedarfsabstufung”

# *Schutzbedarf aus der Betroffenenperspektive formuliert*

- *Normaler Schutzbedarf* besteht für ein Verfahren allein deshalb, weil im Verfahren personenbezogene Daten verarbeitet werden;
- *Hoher Schutzbedarf* besteht wenn ein hohes datenschutzrechtliches Risiko festgestellt wird;
- *Sehr hoher Schutzbedarf* für ein personenbezogenes Verfahren besteht dann, wenn für betroffene Personen Gefahr für Leib und Leben droht.

# *Schutzbedarf entsprechend der Eingriffsintensität für den Betroffenen*

- Ein Datenschutzrisiko ergibt sich nicht erst dadurch, dass eine Organisation eine mehr oder weniger sichere IT nutzt. Das Datenschutzrisiko für einen Betroffenen ist das Verfahren selber! **Der Schutzbedarf ergibt sich insofern aus der Intensität des Grundrechtseingriffs**, wenn eine Organisation ein personenbezogenes Verfahren betreibt.
- Wenn die betriebswirtschaftliche Risikoformel zur Risikoabschätzung herangezogen wird- *"Risiko = Eintrittswahrscheinlichkeit mal Schadenshöhe"* - dann gilt für Datenschutz:
  - Die Eintrittswahrscheinlichkeit der Gefährdung beträgt 100%, denn die Organisation verarbeitet personenbezogene Daten.
  - Schadenshöhe: Ist abzuwägen, insbesondere als ein objektiver Tatbestand, nicht allein als subjektives Ermessen oder als persönlich erlittener Schaden.

# *Maßnahmen entsprechend Schutzbedarfsstufe dimensionieren*

- **Normaler Schutzbedarf**
  Anwendung der Schutzmaßnahmen entsprechend Gewährleistungszielen bereits in der Spezifikationsphase (wg. Art. 25)
- **Hoher Schutzbedarf**
  Anwendung des Katalogs an Schutzmaßnahmen auf sich selber.
  Beispiel in Bezug auf Protokollierung (setzt Transparenz um):
  Protokolldaten leicht zugänglich, durch einen dezidierten Protokollserver integritätsgesichert gespeichert und nur für gesichert Befugte zugänglich sein, rein zweckgesteuerte Auswertungsprozesse sowie Prozesse zur Löschung und Korrektur.
- **Sehr hoher Schutzbedarf**
  wie „hoher Schutzbedarf“ plus individuell abgestimmte zusätzliche Maßnahmen.

# *Angreifermodell des Datenschutzes*

- Der **Hauptangreifer ist die das Verfahren nutzende Organisation** selbst.
- Darüber hinaus gibt es weitere **typische Angreifer-Organisationen** auf Personen, die mittelbar agieren:
  - Sicherheitsbehörden
  - Leistungsverwaltung
  - Bereitsteller von IT-(Infrastruktur)Diensten
  - Bereitsteller kritischer Infrastrukturen (wie Energieversorger)
  - Versicherungen und Banken
  - Forschungsinstitute
  - Krankenhäuser, Ärzte, Dienstleister
  - insbesondere unentschiedene oder untätige Datenschutzaufsichtsbehörden

# SDM-Komponente 3:

# Verarbeitungsbestandteile

# *Verfahrens-komponenten*

Ein personenbezogenes Verfahren besteht aus drei zu betrachtenden Komponenten:

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

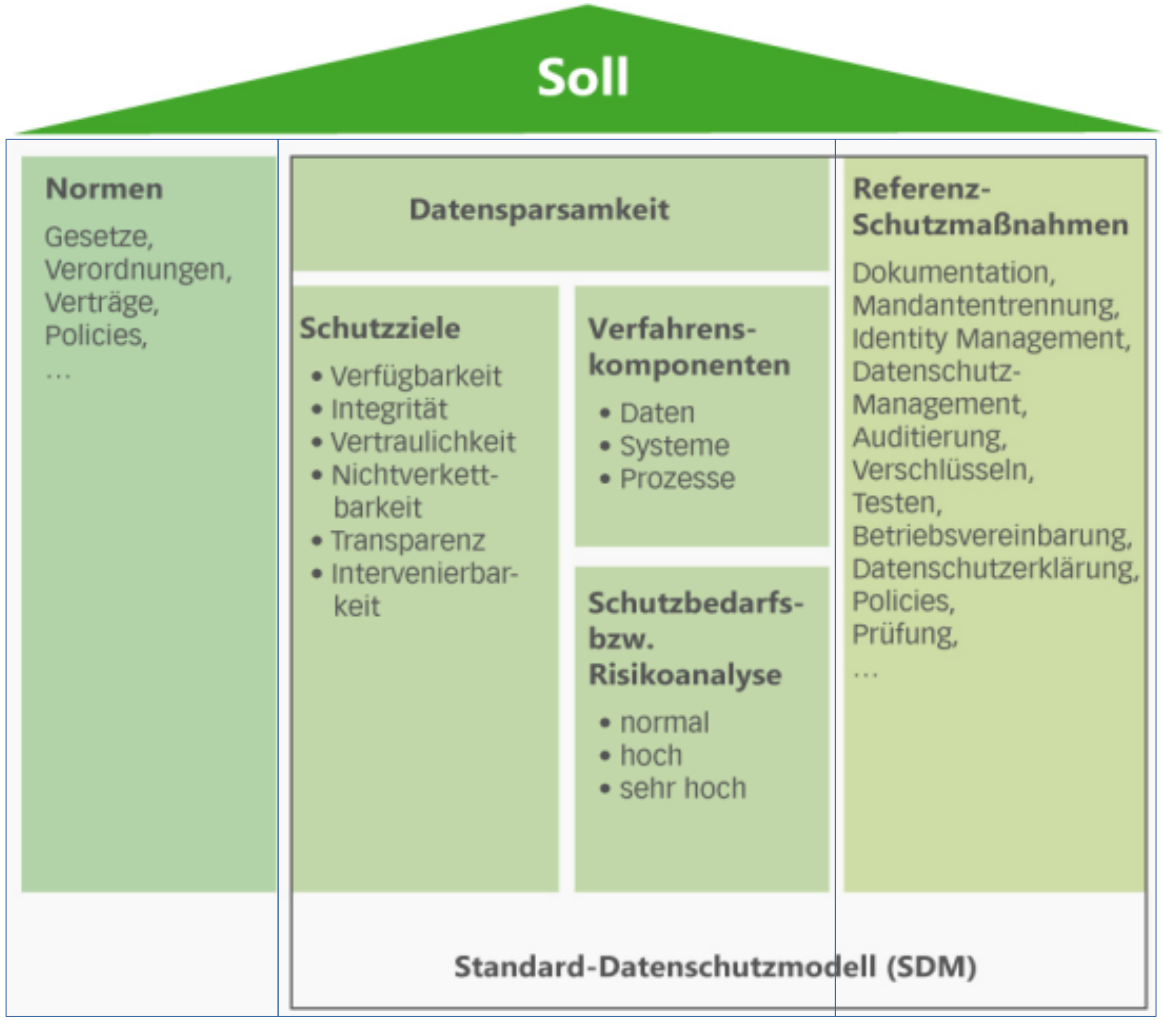
# SDM

# Das gesamte Modell

# Modellierungsidee des SDM: Ausweis spezifischer Referenzschutzmaßnahmen

- 6 + 1 Gewährleistungsziele, verankert in der DSGVO, hinterlegt mit einem Maßnahmen-Katalog für jedes Ziel
- 3 Schutzbedarfsabstufungen (normal, hoch, sehr hoch)
- 3 Verfahrenskomponenten (Daten, Systeme, Prozesse)

Das ergibt eine Matrix mit (theoretisch: 7x3x3) **63** / (praktisch: 6x2x3) **36 Feldern** mit spezifischen Datenschutzanforder-ungen: Für jedes Ziel, jeden Schutzbedarf und jede Komponente muss mindestens eine spezifische Schutzmaßnahme als Referenz festlegbar sein!

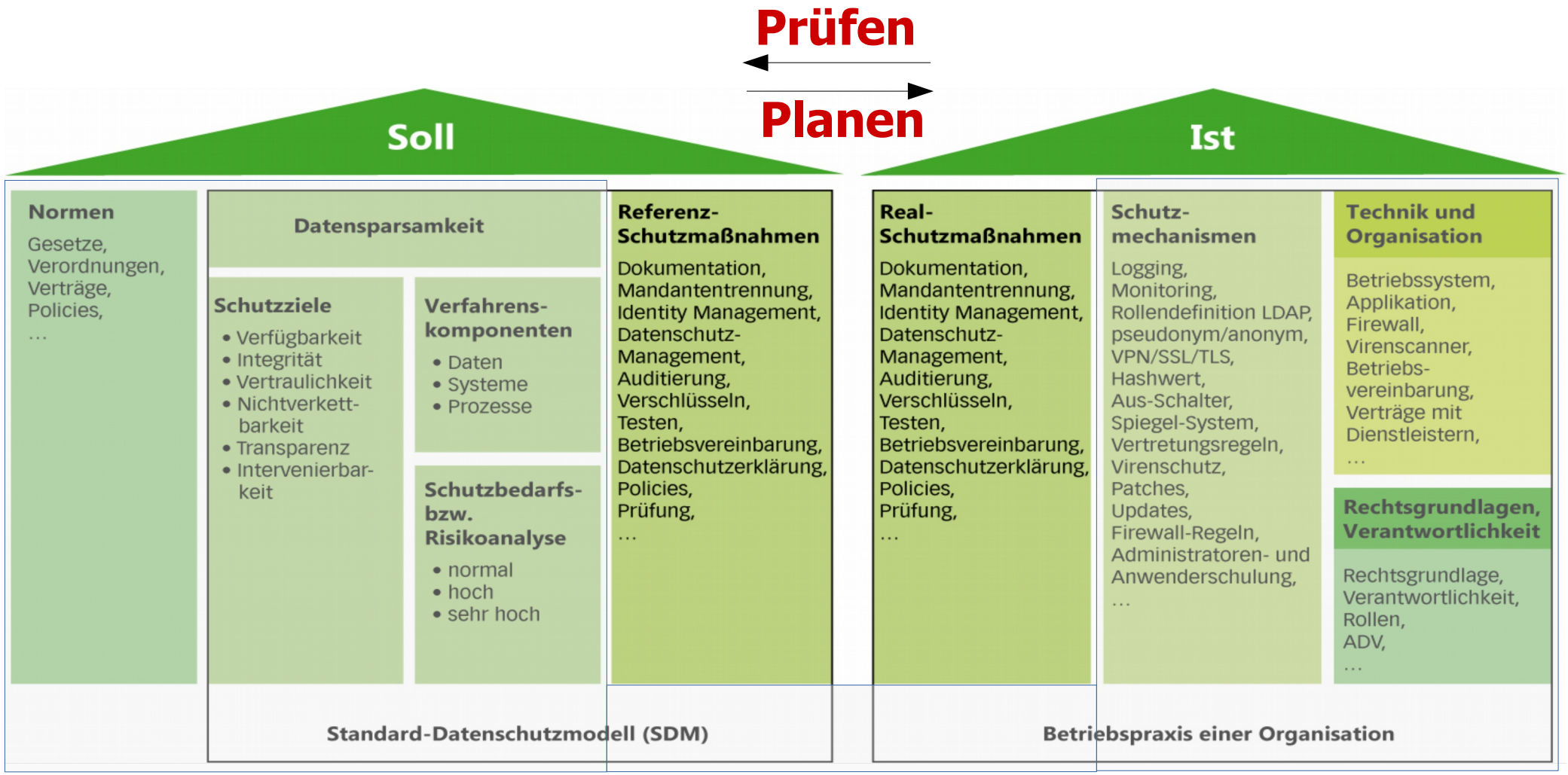



Grafik: M. Rost (ULD)

# SDM
## Ist-Feststellung

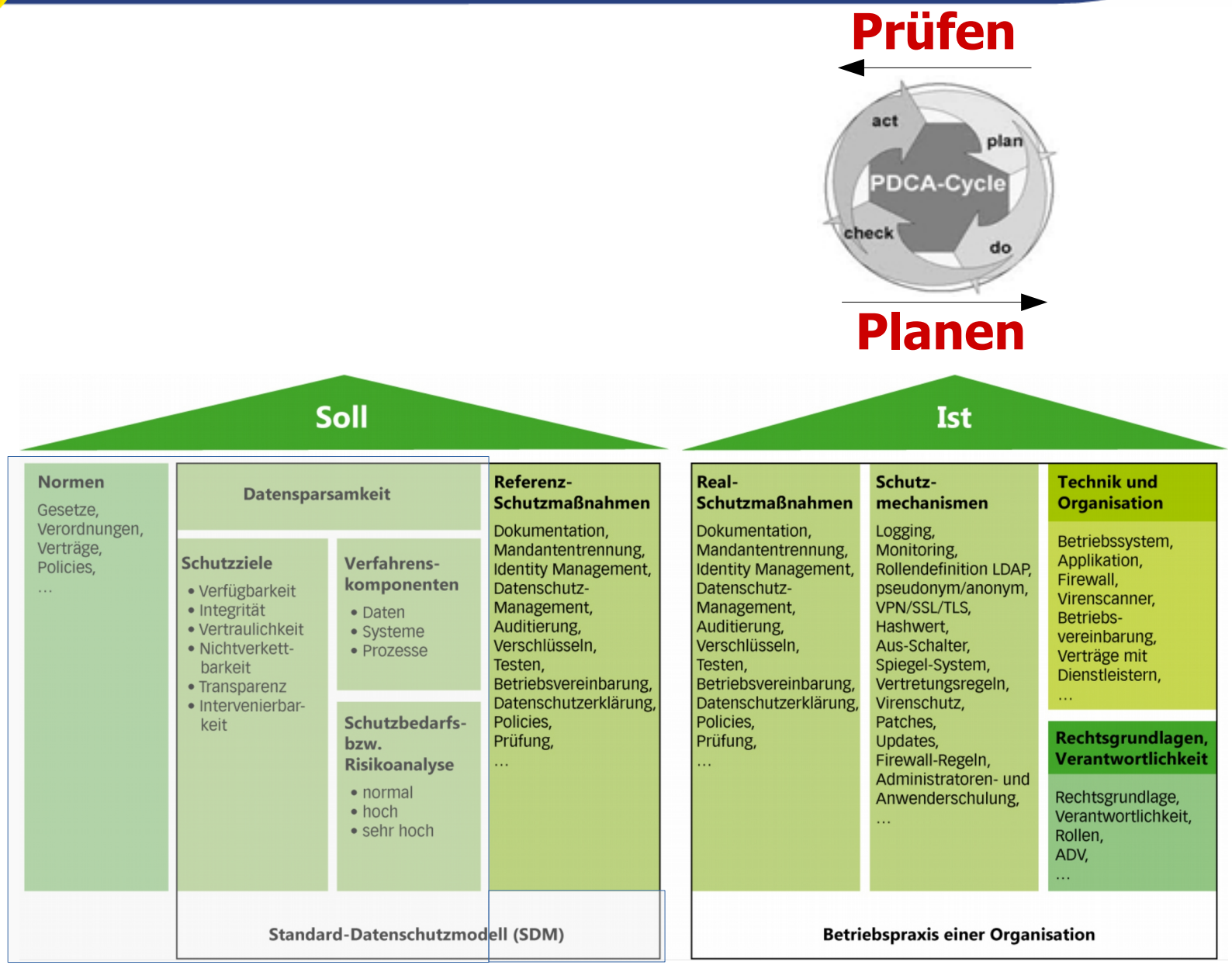

Grafik: M. Rost (ULD)

# Datenschutz prüfen
## Soll-Ist-Bilanz auf Maßnahmenebene




Grafik: M. Rost (ULD)

# Datenschutz-Management mit SDM




Grafik: M. Rost (ULD)

# Beispiel für Maßnahmenkatalog für Schulverwaltungs-SW

(LfD Mecklenburg-Vorpommern)

**1. Entwurf eines Maßnahmenkatalogs für die Einführung einer Schulverwaltungssoftware nach dem Standard-Datenschutzmodell**

| | Daten | | | Gewährleistungsziele | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Schutz-bedarf | Schüler | Erziehungs-berechtigte | Lehrer (Beschäft-igten Daten) | Datensparsamkeit | Verfügbarkeit | Integrität | Vertraulichkeit | Nichtverkettbarkeit | Transparenz | Intervenierbarkeit |
| Normal | Schülernummer | Name | Name | - Rechte- und Rollenkonzept<br><br>- rollen- und aufgabenabhängige Gestaltung der Eingabemasken<br><br>- automatisierte Sperr- und Löschroutinen<br><br>- Möglichkeit der Anbringung von Sperrkennzeichen<br><br>- Möglichkeit der Pseudonymisierung nach Bedarf<br><br>- Möglichkeit der Anonymisierung nach Bedarf<br><br>- vorkonfigurierbare Exportmöglichkeiten für verschiedene Zwecke (z.B. Informationen für Vereine, etc.)<br><br>- landesweit abgestimmtes Softwareänderungs-management | - Rechte- und Rollenkonzept<br><br>- Backup von Daten und Konfiguration nach Backupkonzept<br><br>- Redundanz der zentralen Systeme<br><br>- geeignete dezentrale Backupmaßnahmen (z.B. Papierunterlagen oder Backupleitung…)<br><br>- baulicher Datenschutz (z.B. Brandschutz, Zugangsschutz,…)<br><br>- Schutz vor Schadsoftware<br><br>- Firewall<br><br>- regelmäßige Wartung von Hard- und Software<br><br>- Vertretungs-regelungen für Personal<br><br>- Festlegung von Datenformaten<br><br>- Festlegung der Aufbewahrungsstrategie | - Rechte- und Rollenkonzept<br><br>- Festlegung der jeweils erforderlichen Erfassungsfrequenz der Datenbestände<br><br>- Prüfsummen, Hashverfahren<br><br>- Integritäts-bedingungen für Datenbanken (z.B. Vorgaben für Formate und Wertebereiche)<br><br>- Integritätsschutz für Software (z.B. Signaturen)<br><br>- Protokollierungs-verfahren hinsichtlich der Eingabe und Änderung von Daten | - Rechte- und Rollenkonzept<br><br>- logische Trennung von Schulverwaltungsnetz und Netz für die Lehre<br><br>- zentrale Administration der verwendeten IT-Systeme durch von der verantwortlichen Stelle Beauftragte<br><br>- Zugriff auf die Schulverwaltungssoft ware nur mit Verfahren nach dem Stand der Technik (u.a. Kryptokonzept, Ende-zu-Ende Verschlüsselung, individualisierte Clientzertifikate, sichere Passwortgestaltung)<br><br>- baulicher Datenschutz (z.B. Zugangsschutz)<br><br>- Verpflichtung auf das Datengeheimnis<br><br>- klare vertragliche Regelungen (z.B. Auftragsdatenverarbeitung, Wartungsverträge)<br><br>- Mandanten-trennung bei | - Rechte- und Rollenkonzept<br><br>- Mandanten-trennung bei gemeinsamer Verarbeitung der Daten mehrerer Schulen auf zentralen Datenverarbeitungs anlagen<br><br>-frühestmögliche Anonymisierung und Pseudonymisierung,<br><br>- zweckbezogene Pseudonymisierung<br><br>- Beschränkung der Datenschnittstellen auf das erforderliche Maß<br><br>- Beschränkung der Funktionalität der Software auf das erforderliche Maß<br><br>- bei regelmäßiger Übermittlung von Daten an Dritte ~~durch~~ Bereitstellung eines separaten Abrufdaten-bestandes durch die verantwortliche Stelle | - Rechte- und Rollenkonzept<br><br>- Möglichkeit der Kenntnisnahme von gespeicherten Daten durch den Betroffenen<br><br>- Verfahrens-dokumentationen (u.a. Freigabe, Vorabkontrolle, Verfahrensbeschreibung, Sicherheits-konzept, Verträge, Rechtevergabe, relevante Dienst-anweisungen und Dienstverein-barungen)<br><br>- Dokumentation von Einwilligungen und Widersprüchen (soweit relevant)<br><br>- Dokumentation der Softwareversions-verwaltung und anderer Administrations-handlungen<br><br>- Protokollierungs-verfahren hinsichtlich der Eingabe und Änderung von Daten<br><br>-Auswertungskonzept für Protokolle<br><br>- Protokollierung von | - Rechte- und Rollenkonzept<br><br>- Möglichkeit der Einsicht von Schülern (ggf. Erziehungsberechtigte) in über sie gespeicherte Daten<br><br>- Möglichkeit des Ausdrucks des über den Betroffenen gespeicherten Daten auf Anforderung (z. B. Schülerstammblatt)<br><br>- Einrichtung von Prozessen zur Berichtigung, Sperrung oder Löschung von Daten<br><br>- Rücknahmemöglichkeit von Einwilligungen<br><br>- Einsichtnahmemöglichkeit in Protokolldateien bspw. zu Übermittlungsvorgängen (ggf. gemeinsam mit dem bDSB)<br><br>- Verfahren zur Beauskunftung von Datenübermittlungen (ggf. unter Einbeziehung der Empfänger)<br><br>- Einrichtung von Prozessen zur Information des Betroffenen bei Änderungen von Grunddaten |
| | Name, ggf. Geburtsname | Vorname | Vorname | | | | | | | |
| | Vorname | Anschrift | Anschrift | | | | | | | |
| | Anschrift | Telefon-nummer | Telefon-nummer? | | | | | | | |
| | Telefonnummer | Klassen-elternrat | Geburtsdatum | | | | | | | |
| | Geburtsdatum | | Titel | | | | | | | |
| | Geschlecht | | Funktion | | | | | | | |
| | Geburtsort | | Vertretungs-/Ausfallstunden | | | | | | | |
| | Geburtsland | | | | | | | | | |
| | | | | | | | | | | |
| | **weitere Schülerdaten** | | | | | | | | | |
| | Staatsangehörigkeit | | | | | | | | | |
| | Ausbildungsbetrieb | | | | | | | | | |
| | Einschulungsdatum | | | | | | | | | |
| | bisher besuchte Schulen | | | | | | | | | |
| | zurzeit besuchte Jahrgangsstufe und Klasse gebenenfalls erfolgter Wechsel, Wiederholung, Begrenzung der Verweildauer | | | | | | | | | |
| | Entlassungsdatum | | | | | | | | | |
| | erreichter Abschluss oder Abschlussprüfung | | | | | | | | | |
| | Überweisungsdatum, Name, Anschrift der aufnehmenden Schule | | | | | | | | | |
| | Schwerpunkte bei Ausbildungsgängen (z.B. Fremdsprachenbelegung) | | | | | | | | | |
| | Praktika | | | | | | | | | |
| | Fahrschülerin oder Fahrschüler | | | | | | | | | |
| | Mandat in Mitwirkungsorganen | | | | | | | | | |
| | sonstige schulbezogene Funktionen | | | | | | | | | |
| | Beurlaubung vom Schulbesuch | | | | | | | | | |
| | An-/Abmeldung vom Schulbesuch nach Auslandaufenthalt | | | | | | | | | |
| | Teilnahme an erforderlichen Untersuchungen | | | | | | | | | |
| | | | | | | | | | | |
| | **Leistungsdaten der Schüler mit normalen Schutzbedarf** | | | | | | | | | |
| | Feststellungsprüfung in einer Fremdsprache (Sprache des Herkunftslandes)??? | | | | | | | | | |
| | Kurseinstufungen | | | | | | | | | |
| | Fächer des Wahlpflichtunterrichts | | | | | | | | | |

# SDM-Bausteine (Stand: 2017-04)

## Verfügbarkeit

1. Baustein „Aufbewahrung“
2. Baustein „Datensicherung und -wiederherstellung“

## Integrität

3. Baustein „Ticketsystem und Administrations-Plattform“
4. Baustein „Aspekte eines Datenschutzkonzeptes“

## Vertraulichkeit

5. Entwurf liegt vor, wird aber noch zurückgehalten

## Transparenz

6. Baustein „Spezifikation“
7. Baustein „Dokumentation“
8. Baustein „Protokollierung"
9. Baustein „Auskunft“

## Nichtverkettbarkeit

10. Baustein „Anonymisierung & Pseudonymisierung“
11. Baustein „Trennung“
12. Baustein „Rollen und Berechtigungen“

## Intervention

13. Baustein „Berichtigung“
14. Baustein „Löschen“
15. Baustein „Sperren“
16. Baustein „Single Point of Contact (SPoC)“

# *SDM-Bausteine (Stand: 2017-04)*

**Es fehlen Bausteine zu den Themen:**

- *„Kryptoverfahren“* (Verschlüsselung / Integritätssicherung)
  Status: Entwurf im frühen Stadium
- *„Umsetzung von Datensparsamkeit“*
- Status: Entwurf in Diskussion

**Weitere im Kontext des SDM entstandene Bausteine:**

- *„Datenschutz-Folgenabschätzung“*
  Status: Ist kein Bestandteil des SDM, sondern wird eine Orientierungshilfe
- *„Datenschutz-Zuständigkeiten (Datenschutzbeauftragter)“*
  Status: Ist kein Bestandteil des SDM, sondern wird eine Orientierungshilfe

# SDM-Bausteine Aufbau der Texte (Stand: 2017-04)

**Baustein …**

*1 Bezug zu Gewährleistungszielen*

*2 Darstellung und Zweck*

Daten

Technische Systeme

Prozesse

*3 Differenzierung bei hohem Schutzbedarf*

*4 Referenzen*

*5 Zusammenfassung der Maßnahmen*

Ebene Daten

M D01 …

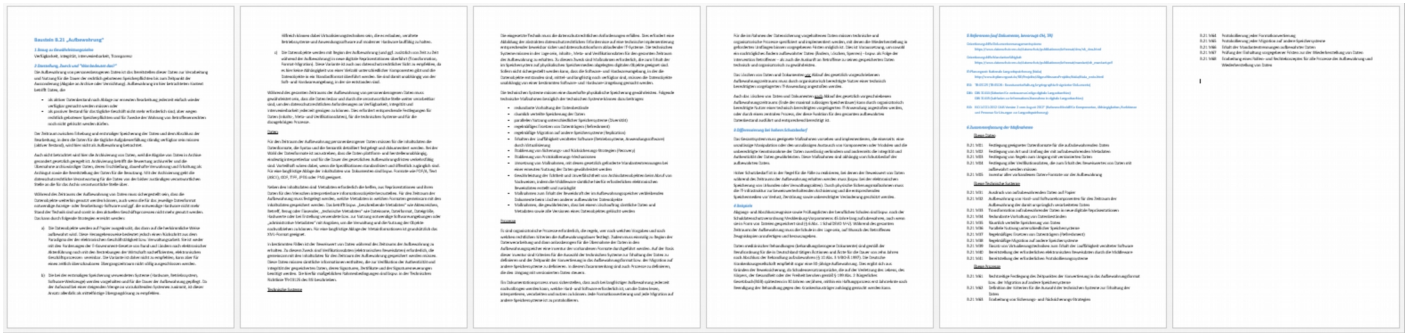
Ebene Technische Systeme

M T01 …

Ebene Prozesse

M P01 …

1) Bezug zu Gewährleistungszielen
2) Darstellung und Zweck
   - Daten
   - technische Systeme
   - Prozesse
3) Differenzierung bei hohem Schutzbedarf
4) Referenzen
5) Zusammenfassung der Maßnahmen



# Agenda

1. Was meint „Datenschutz“?
2. Objektbereich des Datenschutzes
3. Datenschutz-Risiken
4. Komponenten des Standard-Datenschutzmodells (SDM)

**5. Beispiele: Protokollierung nach SDM / Datenschutz Folgenabschätzung mit SDM”**

6. Zum nicht unproblematischen Verhältnis von Informationssicherheit und operativem Datenschutz
7. Referenzen und Kontakt

# *Beispiel 1 für einen SDM-Maßnahmebaustein: Protokollierung*

- Protokollierung ist eine Umsetzung des **Schutzziels „Transparenz“**.

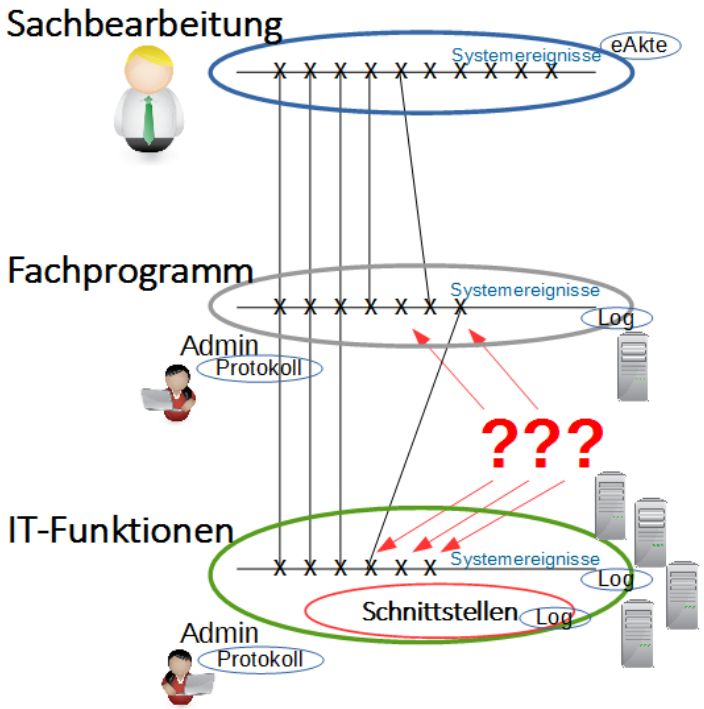
- Zweck der Protokollierung:
  „Die Protokollierung ist eine Schutzmaßnahme, um fachliche, technische, organisatorische und administrative Aktivitäten und Entscheidungen, die in der **Vergangenheit** stattfanden, aufzuklären.“ (SDM-Handbuch, V1.0)

- Dem Verantwortlichen (ehemals „verantwortliche Stelle“) dient Protokollierung (neben „Spezifikation“ und „Dokumentation“) als **Nachweis der Gesetzeskonformität des Organisationshandelns** (vgl. Art. 5 / Art. 24 / Art. 35 „Nachweispflicht“).
  Die Folge? Protokollierung wird selber zu einer „Verarbeitung“.

# *Inhalte einer Protokollierung*

1. Zeitkomponente (**Wann**?)
2. Instanz, die eine Aktivität auslöst (**Wer**?)
3. Aktivität bzw. Ereignis, das durch die Instanz ausgelöst wurde (**Was**?)
4. die Adresse der Speicherinstanz, die diese Protokolldaten speichert (**Durch wen protokolliert**?).

# Zu protokollierende Systemebenen

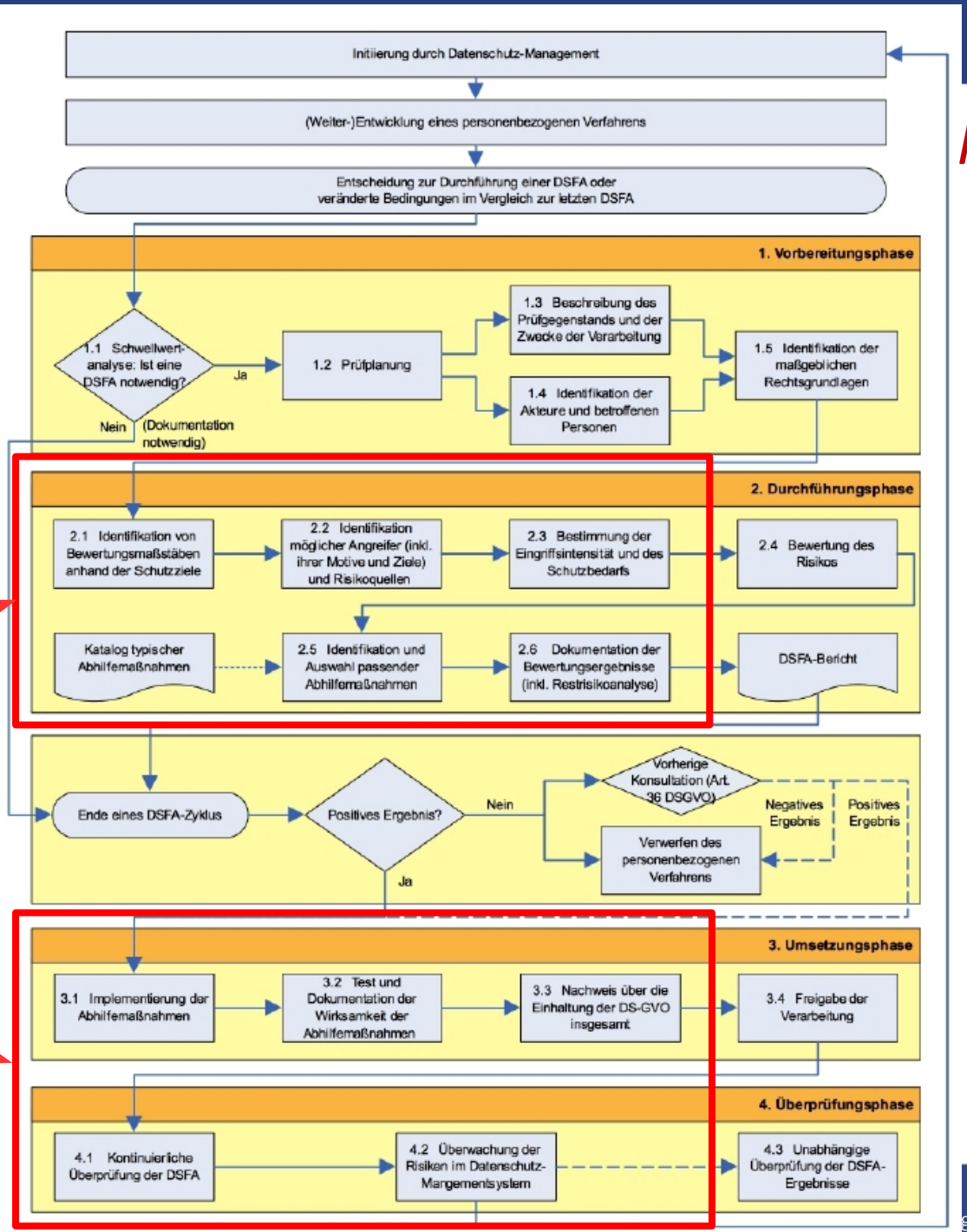



1. Die Aktivitäten der **Sachbearbeitung**;
2. die **Funktionen des Fachprogramms** für die Sachbearbeitung;
3. die **Administration des Fachprogramms**;
4. die **IT-Funktionen der Infrastruktur** (Hardware, Software)
   einer Organisation, auf denen die Fachprogramme aufsetzen (PCs, Server, virtuelle Systeme, Betriebs-systeme, Middleware/DB, CPU-Cluster, SAN/NAS)-
   **Sonderfunktionalität**: Schutzmaßnahmen (Hashen, Verschlüsseln, Anonymisieren...) des Datenschutzes und der IT-Sicherheit;
5. die **Systemschnittstellen**, Übermittlung von Daten zu anderen Organisation(seinheit)en;
6. die **Administration der IT-Infrastruktur und Systemschnittstellen.**

7. Und ebenso ist zu protokollieren, ob ein Controlling dieser Protokolle stattgefunden hat. (Erst das kann zum Nachweises der Wirksamkeit auch der Protokollierung genutzt werden).

Grafik: M. Rost (ULD)

# Beispiel 2: Datenschutz-Folgenabschätzung mit SDM




SDM
Standard-Datenschutzmodell

1. Vorbereitung (*Plan*)

2. Durchführung (*Do*)

3. Umsetzung (*Act*)

4. Überprüfung (*Check*)

Quelle:
Forum Privatheit: Whitepaper **Datenschutz-Folgenabschätzung**; V3.0

# Agenda

1. Was meint „Datenschutz“?
2. Objektbereich des Datenschutzes
3. Datenschutz-Risiken
4. Komponenten des Standard-Datenschutzmodells (SDM)
5. Beispiele: Protokollierung nach SDM / Datenschutz Folgenabschätzung mit SDM”

**6. Zum nicht unproblematischen Verhältnis von Informationssicherheit und operativem Datenschutz**

7. Referenzen und Kontakt

# *Zum Verhältnis Informationssicherheit/Grundschutz und operativer Datenschutz/SDM*

*Bis 2000*:

**Datenschutz dominiert Datensicherheit wg. Datenschutzrecht**

Datensicherheit entspricht operativem Datenschutz. Geld für erste Schutzmaßnahmen werden mit dem Datenschutzrecht begründet, einige DSBe können IT ein bißchen prüfen.

*Zwischen 2000 und 2012*:

**IT-Sicherheit dominiert den operativen Datenschutz aufgrund wesentlich besserer Methoden**

Verhältnis IT-Sicherheit und operativer Datenschutz ist schlecht konturiert, das Thema Sicherheit kommt langsam im Management an, einige Datenschutz-Experten werden zu IT-Beratern.

# Operativer Datenschutz
## Datensicherheit, IT-Sicherheit, Informationssicherheit

*Ab 2012*:

- **Separierung Datenschutz und Datensicherheit**, Datenschutz entwickelt spezifische Schutzmaßnahmen (z.B. nutzerkontrolliertes Identitymanagement, Anonymisierung, Protokollierung);
- **IT-Sicherheit bekommt zunehmend eigene gesetzliche Grundlagen** (bspw. De-Mail, nPA, IT-Sicherheitsgesetz, IT-Sicherheitsleitlinie für die deutsche Verwaltung, Kritische Infrastrukturen), der DSB wird zum Verbündeten gegenüber der Leitung aber zum Risiko bei den Sicherheitsmaßnahmen; starke Professionalisierung
- **Operativer Datenschutz zieht methodisch an → SDM** der IT-SiBe bzw. Informationssicherheit wird zu einem eigenen Typ von Datenschutzrisiko; grundrechtlich begründeter Primat des Datenschutzes (wg. Art. 1).

Rollen-Differenzierungen in der Informationssicherheit:

- Sicherheitsmanager für Gefahren- und Risikoanalysen
- Security-Architekt
- IT-Security-Manager
- IT-Security-Officer
- Consultant für IT-Security-Lösungen
- IT-Security-Analyst
- Cyber-Security-Analytiker
- IoT Engineer für Cloud-Security

**Wo sind die differenzierten Rollen im Datenschutz?**

# Stellung der Sicherheits-Experten in den Organisationen ist stark geworden

**Jahresbruttogehälter von IT-Fachkräften 2017**

| Bereich | Durchschnitt 2017 | Durchschnitt 2016 |
|---|---|---|
| IT-Sicherheit | 75 000 € | 71 000 € |
| IT-Projektleitung | 73 000 € | 70 000 € |
| SAP-Beratung | 72 000 € | 69 000 € |
| IT-Leitung | 72 000 € | 69 000 € |
| IT-Beratung, Analyse, Konzeption | 68 000 € | 67 000 € |
| SAP-Entwicklung | 65 000 € | 60 000 € |
| Softwareentwicklung Backend | 58 000 € | 57 000 € |
| Software / gesamte EDV | 57 000 € | 57 000 € |
| Softwareentwicklung Mobile | 56 000 € | 54 700 € |
| UX User Experience | 54 700 € | 56 000 € |
| DV-Schulung | 52 000 € | 54 000 € |
| Datenbankadministration | 50 000 € | 46 000 € |
| Softwareentwicklung Frontend | 49 000 € | 43 000 € |
| System- und Netzwerk-administration | 48 000 € | 49 000 € |
| Anwendersupport | 42 000 € | 43 000 € |
| Webdesign, Webprogrammierung | 37 000 € | 37 000 € |

Beträge auf volle 1000 Euro gerundet

Quelle: iX 2018, Nr. 3, S. 39

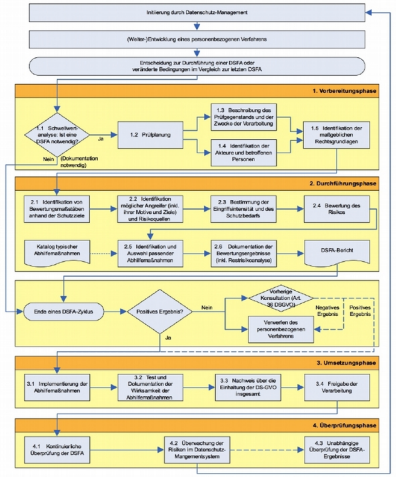
Jahresbruttogehalt IT-Sicherheits-Experte: 75.000 Euro

In den meisten Fällen gilt rechtlich: **Datenschutz führt,** der DSB hat den Lead!
Aber: **Beeindruckt das einen IT-Sicherheits-Experten?**

# Literaturhinweise

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

Forum Privatheit: Whitepaper **Datenschutz-Folgenabschätzung**
https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf



**DSBK 2016: Handbuch zur SDM-Methodik, V1.0**
https://www.datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf


**SDM-Newsletter** der UAGSDM:
https://www.datenschutzzentrum.de/sdm/
[Link unten: „Newsletter“]

**Schulungen zum SDM:**
regelmäßig bei der DSA: https://www.datenschutzzentrum.de/akademie/

# *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/