Wie führt man eine Datenschutz-Folgenabschätzung in der öffentlichen Verwaltung systematisch durch?

Martin Rost

16.04.2018, Weimar

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

SDM
Standard-Datenschutzmodell

IT-Planungsrat

Agenda

1. Was meint „Datenschutz“?

2. Wann ist eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen (Art. 35 DSGVO)?

3. Wie ist eine Schwellwert-Analyse für eine DSFA durchzuführen (Art. 24 DSGVO)?

4. Wie lässt sich eine Datenschutz-Folgenabschätzung durchführen (DSFA-Framework, V3.0)?

5. Wie lassen sich Datenschutz-Schutzmaßnahmen zur Verringerung von Risiken bestimmen (Standard-Datenschutzmodell (SDM), V1.0)?

6. Referenzen

Agenda

1. Was meint „Datenschutz“?

2. Wann ist eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen (Art. 35 DSGVO)?

3. Wie ist eine Schwellwert-Analyse für eine DSFA durchzuführen?

4. Wie lässt sich eine Datenschutz-Folgenabschätzung durchführen? (DSFA-Framework, V3.0)

5. Wie lassen sich Datenschutz-Schutzmaßnahmen zur Verringerung von Risiken bestimmen? (Standard-Datenschutzmodell (SDM))

6. Referenzen

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.

- **Datenschutz gründet nicht im individuellen Bedürfnis nach Privatheit.**

  Konzepte wie “Selbstbestimmung”, “Privatautonomie”, „individuelle Grundrechte“ sind in modernen Gesellschaften funktionale Voraussetzungen für deren Funktionieren.

Der Objektbereich des Datenschutzes

Datenschutz beobachtet, beurteilt und gestaltet die asymmetrischen Machtbeziehungen zwischen Organisationen und Personen... aus der Perspektive des **Risikonehmers "Person"** und dem **Risikogeber "Organisation"**.

Verhältnis IT-Sicherheit – Datenschutz

IT-Sicherheit unterstellt methodisch:
Jede Person kann ein Angreifer sein!

Was unterstellt Datenschutz methodisch?

Datenschutz unterstellt methodisch:
Jede Organisation ist ein Angreifer!

(Für Kryptologen: Bob insbesondere ist der Angreifer!)

DER datenschutzrechtliche Grundsatz des kontinentaleuropäischen Datenschutzrechts lautet:

Organisationen dürfen keine personen-bezogenen Daten verarbeiten PUNKT

„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 seit 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. ← Grundrecht auf Datenschutz

(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. ← Verbot mit Erlaubnisvorbehalt
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. ← Datenschutzkontrolle

Risiken im Datenschutz

- Das spezifische operative Datenschutz-Risiko besteht darin, dass die "**Intensität der Beeinträchtigungen für die Rechte und Freiheiten natürlicher Personen"** (deutsch: "Grundrechtseingriff") **durch Organisationen nicht auf ein zumindest ausreichendes 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 und diese löschen oder verändern können.

Agenda

1. Was meint „Datenschutz“?

2. Wann ist eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen (Art. 35 DSGVO)?

3. Wie ist eine Schwellwert-Analyse für eine DSFA durchzuführen?

4. Wie lässt sich eine Datenschutz-Folgenabschätzung durchführen? (DSFA-Framework, V3.0)

5. Wie lassen sich Datenschutz-Schutzmaßnahmen zur Verringerung von Risiken bestimmen? (Standard-Datenschutzmodell (SDM))

6. Referenzen

Datenschutz-Folgenabschätzung (Art. 35 / EG 84, 89-93 DSGVO)

1. **Eine Datenschutz-Folgenabschätzung (DSFA) bzw. ein Data-Protection-Impact-Assessment (DPIA) ist für eine Verarbeitung durchzuführen** bei:
   1. „hohem Risiko“, und wenn eine Verarbeitung auf der Muss-Liste der Aufsichtsbehörden steht;
   2. Scoring, Profiling, automatisiertem Einzelentscheid, Videoüberwachung öffentlichen Raums;
   3. besonders schutzwürdigen Daten (z.B. nach Art. 9 DSGVO)
2. **Bestandteile** einer DSFA:
   1. Beschreibung des Verfahrens, der Zwecke, der berechtigten Interessen sowie eine Bewertung der Notwendigkeit der DV, der Verhältnismäßigkeit und der Risiken für Betroffene;
   2. Beschreibung der geplanten Schutzmaßnahmen inkl. Nachweis über deren Wirksamkeit;
   3. Extern auditierte Verfahren und Audits
   4. Standpunkte der Betroffenen;
3. Der/die **Datenschutzbeauftragte** ist nicht verantwortlich, auch keine abschließende Beurteilung
4. Der **Verantwortliche** muss am Ende den Betrieb des Verfahrens prüfen.

Objekt zur Durchführung einer Datenschutz-Folgenabschätzung 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

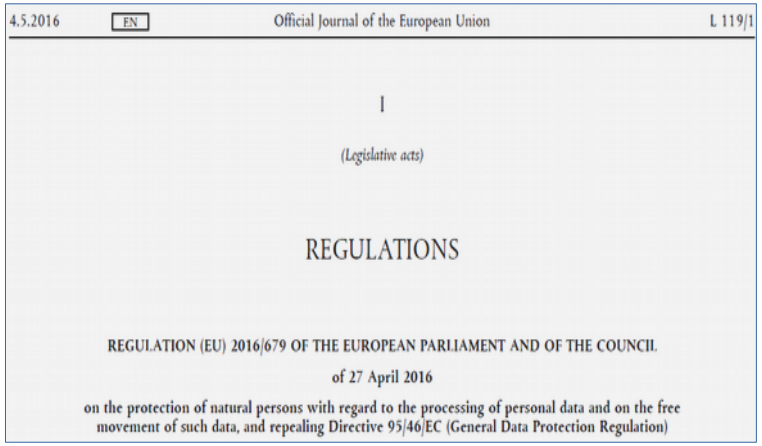
- das Erheben,
- das Erfassen,
- die Organisation,
- das Ordnen,
- die Speicherung,
- die Anpassung oder Veränderung,
- das Auslesen,
- das Abfragen,
- die Verwendung,
- die Offenlegung durch Übermittlung,
- Verbreitung oder eine andere Form der Bereitstellung,
- den Abgleich oder die Verknüpfung,
-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

Verarbeitung

Eine Verarbeitung...

- ist eine Aktivität einer **Organisation**;
- hat einen **Verantwortlichen**;
- wird bestimmt durch einen **Zweck** (oder mehrere kompatible Zwecke);
  - Zwecksetzung (*Ist die Verarbeitung legitim?*)
  - Zweckbeschreibung oder Zweckdefinition (*Ist die Verarbeitung legal?*)
  - Zwecktrennung (*Wo liegt bei der Verarbeitung der operative Kurzschluss?*)
  - Zweckbindung (*Ist die Zb im Verfahren horizontal im Fachverfahren, vertikal über alle IT-Ebenen und Prozesse hinweg sichergestellt?*)
- ist in der Regel als Sachbearbeitung mit den Komponenten **Daten, IT-Systemen und Prozessen** implementiert.

Operative Prüfgrößen der DSGVO für Risikobestimmungen



4.5.2016 EN Official Journal of the European Union L 119/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- **Art. 5**: „***Grundsätze*** für die Verarbeitung personenbezogener Daten“
- **Art. 9**: „Verarbeitung ***besonderer Kategorien*** personenbezogener Daten“
- Art. 12-23: „Rechte der Betroffenen“
- **Art. 24**: „Verantwortung des für die Verarbeitung Verantwortlichen, ***Risikobestimmung***“
- Art. 25: „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“
- Art. 32: „Sicherheit personenbezogener Daten“
- **Art. 35**: ***„Datenschutz-Folgenabschätzung“***
- Art. 36: „vorherige Konsultation“

Abs. 10: Durchführung DSFA ist bereits im Rahmen einer Gesetzgebung möglich

„(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln ***und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte****, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.“*

Agenda

1. Was meint „Datenschutz“?

2. Wann ist eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen (Art. 35 DSGVO)?

3. Wie ist eine Schwellwert-Analyse für eine DSFA durchzuführen?

4. Wie lässt sich eine Datenschutz-Folgenabschätzung durchführen? (DSFA-Framework, V3.0)

5. Wie lassen sich Datenschutz-Schutzmaßnahmen zur Verringerung von Risiken bestimmen? (Standard-Datenschutzmodell (SDM))

6. Referenzen

Datenschutz-Risiko

Komponenten der Risikoformel aus Art. 24 DSGVO

„(1) Der Verantwortliche setzt unter Berücksichtigung der **Art**, des **Umfangs**, der **Umstände** und der **Zwecke** der **Verarbeitung** sowie der unterschiedlichen ***Eintrittswahrscheinlichkeit*** *und* ***Schwere*** *der* ***Risiken*** für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.“

Verfahrenseigenschaften → wann besteht hohes Risiko?

- **Art** → wenn Daten sensibel, IT-Systeme unsicher, Prozesse undefiniert sind
- **Umfang** → wenn massenhafte Betroffenheit besteht
- **Umstände** → wenn sensible Kontexte (Abhängigkeiten)
- **Zwecke** → wenn Verfahren keine hinreichende legitime Zwecksetzung/ praktikable Zweckbindung aufweisen

Risikoformel der DSGVO für Rechte und Freiheiten:

Eintrittswahrscheinlichkeit x Schwere des Schadens = Risiko

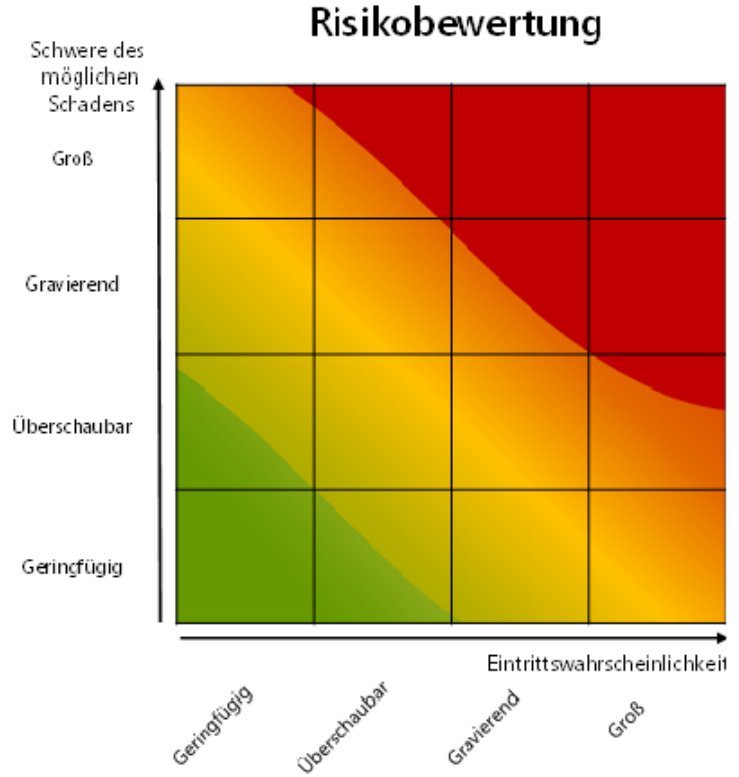
- Eintrittswahrscheinlichkeit → 100%
- Schwere des Schadens → Grundrechtseingriff

„Schäden“ gemäß Art. 24 DSGVO

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

Erwägungsgrund 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.



Art. 9

„Verarbeitung besonderer Kategorien personenbezogener Daten“

„(1) Die Verarbeitung personenbezogener Daten, aus denen **die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit** hervorgehen, sowie die Verarbeitung von **genetischen Daten, biometrischen Daten** zur eindeutigen Identifizierung einer natürlichen Person, **Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung** einer natürlichen Person ist untersagt.“

Kriterien für DSFA gem. WP248 der Art. 29 Gruppe

(a) Vertrauliche oder höchst persönliche Daten

(b) Daten zu schutzbedürftigen Betroffenen (Kinder, Kranke, Gefange...)

(c) Datenverarbeitung in großem Umfang

(d) Systematische Überwachung

(e) Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen

(f) Bewerten oder Einstufen (Scoring)

(g) Abgleichen oder Zusammenführen von Datensätzen (Verschneiden)

(h) Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung

(i) Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert

„Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679“ – 4.10.2017

Status der Muss-Liste Art. 35, Abs. 4 DSGVO

- Der Entwurf der Muss-Liste der deutschen Datenschutz-Aufsichtsinstanzen umfasst aktuell 5 Kriterien pro erfasster Verarbeitung:
  1. Allgemeine Bezeichnung der **Verarbeitungstätigkeit** (z.B. „*Scoring durch Auskunfteien, Banken oder Versicherungen*“)
  2. **Beispiel** („*Eine Bank führt Scoring durch, um die Höhe des Zinssatzes bei einem Kreditvertrag für Bankkunden zu bestimmen.*“)
  3. Ausweis der **Kriterien des WP248**-Papers der Art. 29-Gruppe*
  4. Ausweis **zusätzlicher Kriterien** aus dem deutschen Aufsichtsbereich
  5. Bereich: **öffentlich / privat**
- Ein Entwurf für die Verwaltung der **Muss-Liste im Normalbetrieb** (bspw. mit Regelungen für Eintragenlassen/ Austragenlassen, Versionierung der Muss-Liste, Publikationsort, Publikationsformats) liegt vor.
- Unklar ist, ob die Muss-Liste von zuständiger Aufsichtsbehörde, deutschlandweit oder EU-weit publiziert werden wird.

*„Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679“ – 4.10.2017

Agenda

1. Was meint „Datenschutz“?

2. Wann ist eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen (Art. 35 DSGVO)?

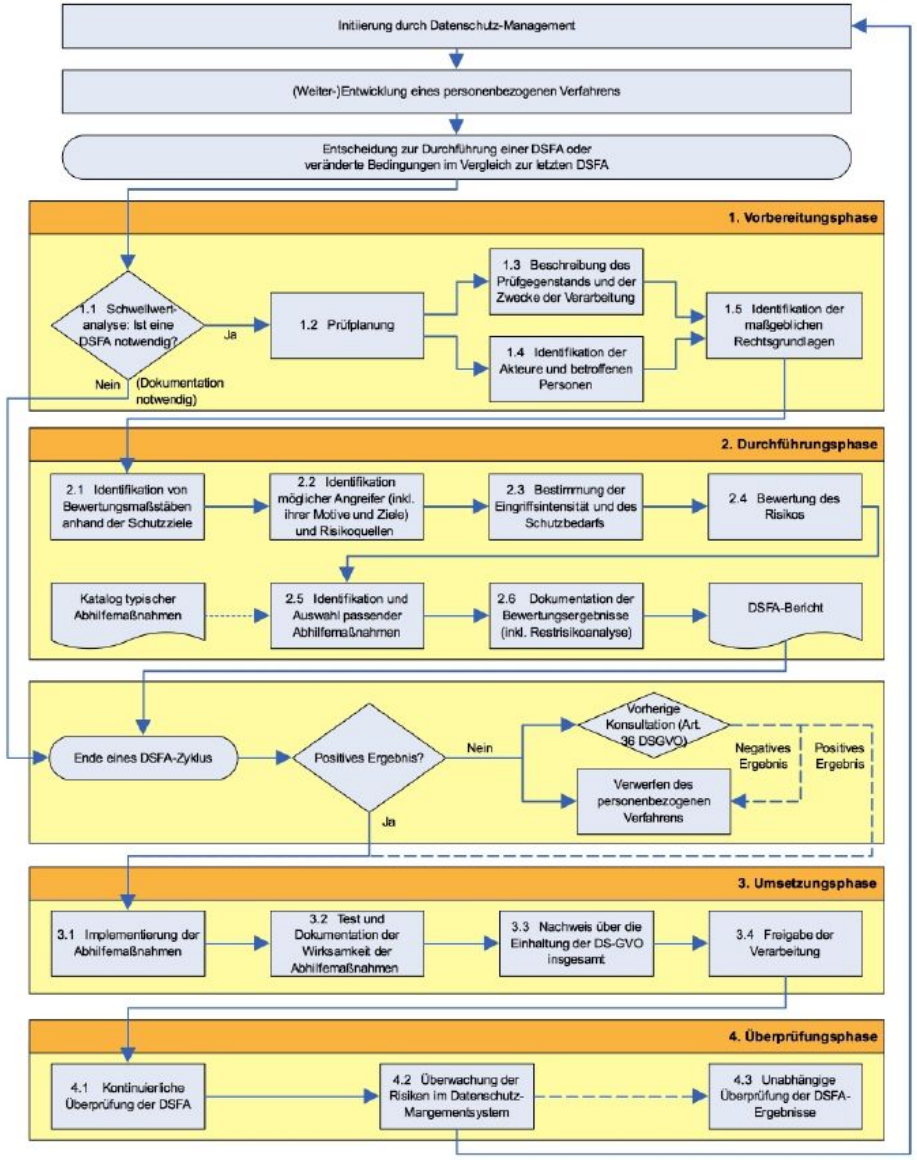
3. Wie ist eine Schwellwert-Analyse für eine DSFA durchzuführen?

4. Wie lässt sich eine Datenschutz-Folgenabschätzung durchführen? (DSFA-Framework, V3.0)

5. Wie lassen sich Datenschutz-Schutzmaßnahmen zur Verringerung von Risiken bestimmen? (Standard-Datenschutzmodell (SDM))

6. Referenzen

DSFA durchführen
Whitepaper-Framework, V3.0



Quelle:
Forum Privatheit: Whitepaper
Datenschutz-Folgenabschätzung, V3.0

Autoren:
- Fraunhofer ISI, Karlsruhe
- Institut Wirtschaftsrecht, Uni Kassel
- DS-Aufsichtsbehörde: ULD, Kiel

Agenda

1. Was meint „Datenschutz“?

2. Wann ist eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen (Art. 35 DSGVO)?

3. Wie ist eine Schwellwert-Analyse für eine DSFA durchzuführen?

4. Wie lässt sich eine Datenschutz-Folgenabschätzung durchführen? (DSFA-Framework, V3.0)

5. Wie lassen sich Datenschutz-Schutzmaßnahmen zur Verringerung von Risiken bestimmen? (Standard-Datenschutzmodell (SDM))

6. Referenzen

Standard-Datenschutzmodell (SDM)

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.

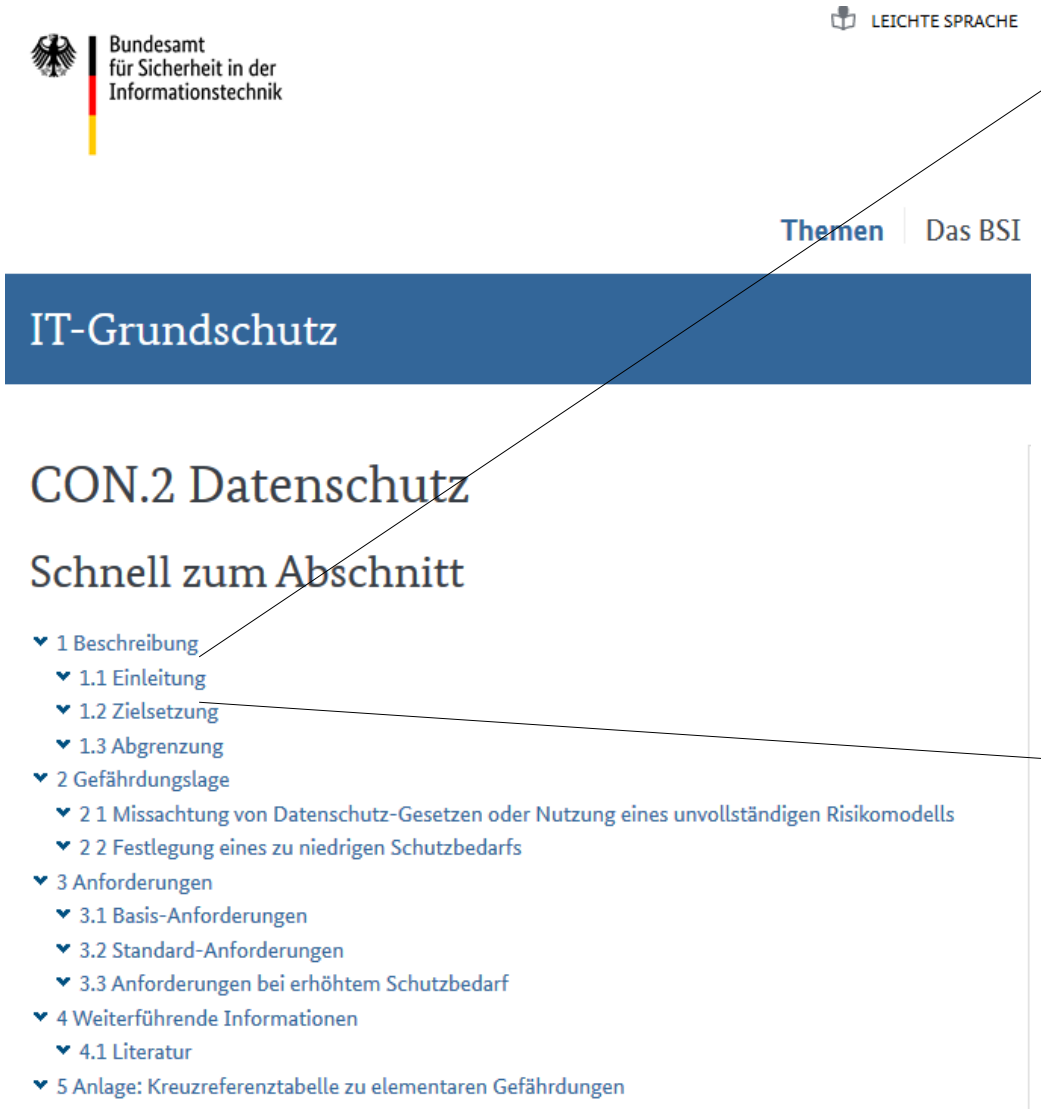
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat ihre Kontroll- und Beratungspraxis auf eine systematische und konsistente Grundlage gestellt. Auch hatten sie vielfach Kritik an Innenminister parat.

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

- **Vermittelt Recht und Technik** und benennt Schutzmaßnahmen.
- **Normative Verankerung in der DSGVO.**
- Die deutschen Datenschutz-Aufsichtsbehörden haben 2016/11 die **SDM-Methodik** festgelegt.
- Kernteam umfasst ca. 8 Personen aus verschiedenen Aufsichtsbehörden als Unterarbeitsgruppe (**UAGSDM**) des Arbeitskreis-Technik der DSB-Konferenz.
- **Betriebskonzept**:
  - Bausteine werden nur durch DS-Aufsichtsbehörden erstellt
  - Qualitätsmanagemente durch Reviews innerhalb UAGSDM und AK-Technik
- Handbuch ist auf den **Webseiten** der deutschen Datenschutzaufsichts-behörden publiziert, am 25.4. steht die V1.1 zur Abstimmung.
- Methodische **Anlehnung an Grundschutz**, IT-Grundschutz des BSI verweist im DS-Baustein CON2 auf das SDM (SDM ersetzt Datenschutzbaustein M1.5)
- Kap. 7 des Handbuchs listet generische **Maßnahmen** auf.
- Sachsen, Mecklenburg-V., Hessen, Schleswig-H., Evangelische Kirche Deutschland werden **Bausteinekatalog in Eigenregie ab Juni 2018 publizieren.**

IT-Grundschutz und SDM



Bundesamt für Sicherheit in der Informationstechnik

LEICHTE SPRACHE

Themen | Das BSI

IT-Grundschutz

CON.2 Datenschutz

Schnell zum Abschnitt

- 1 Beschreibung
  - 1.1 Einleitung
  - 1.2 Zielsetzung
  - 1.3 Abgrenzung
- 2 Gefährdungslage
  - 2 1 Missachtung von Datenschutz-Gesetzen oder Nutzung eines unvollständigen Risikomodells
  - 2 2 Festlegung eines zu niedrigen Schutzbedarfs
- 3 Anforderungen
  - 3.1 Basis-Anforderungen
  - 3.2 Standard-Anforderungen
  - 3.3 Anforderungen bei erhöhtem Schutzbedarf
- 4 Weiterführende Informationen
  - 4.1 Literatur
- 5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

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.“

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

IT-Grundschutz "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.

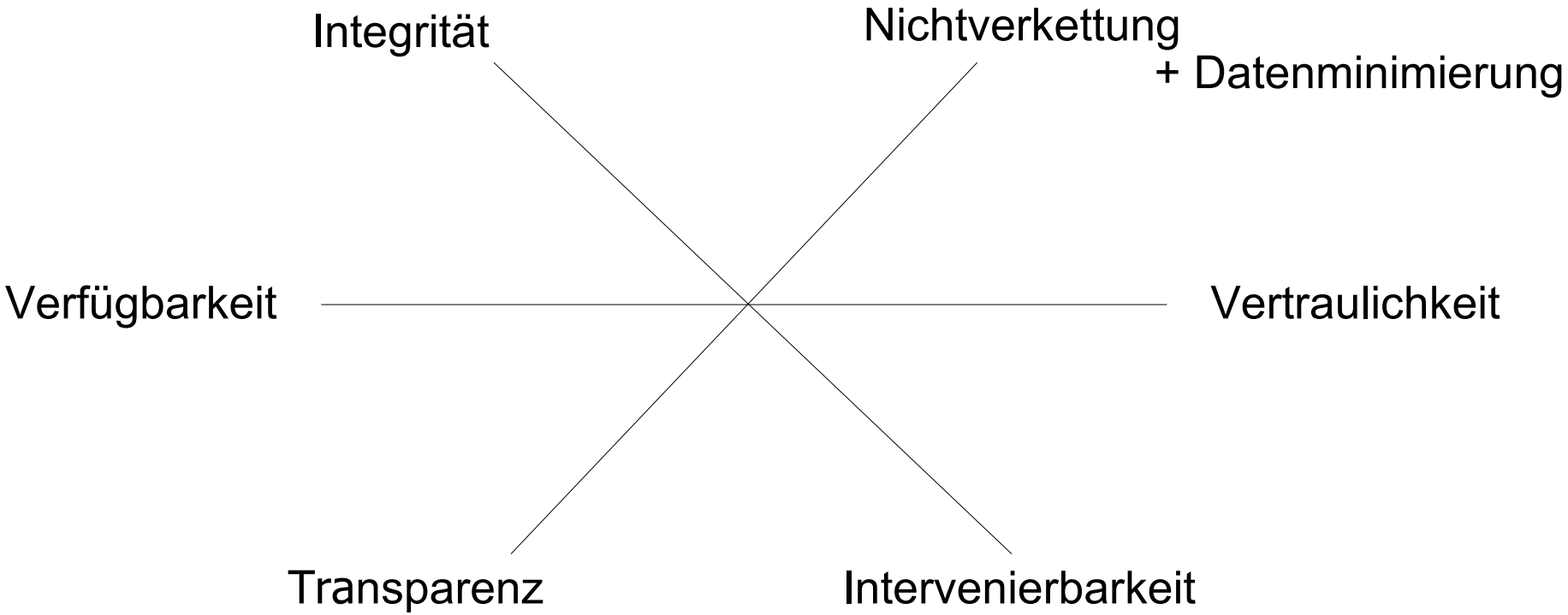
Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_2_Datenschutz.html

Aufbau des Modells

SDM-Komponente 1:

“Gewährleistungsziele”

Systematik der elementaren Gewährleistungsziele des SDM



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

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

SDM-Bausteine für Schutzmaßnahmen zur Umsetzung der Gewährleistungsziele

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-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 ein sehr hohes Risiko für betroffene Personen mit Gefahr für Leib und Leben droht.

SDM-Komponente 3:

Verarbeitungsbestandteile

Verfahrens-komponenten

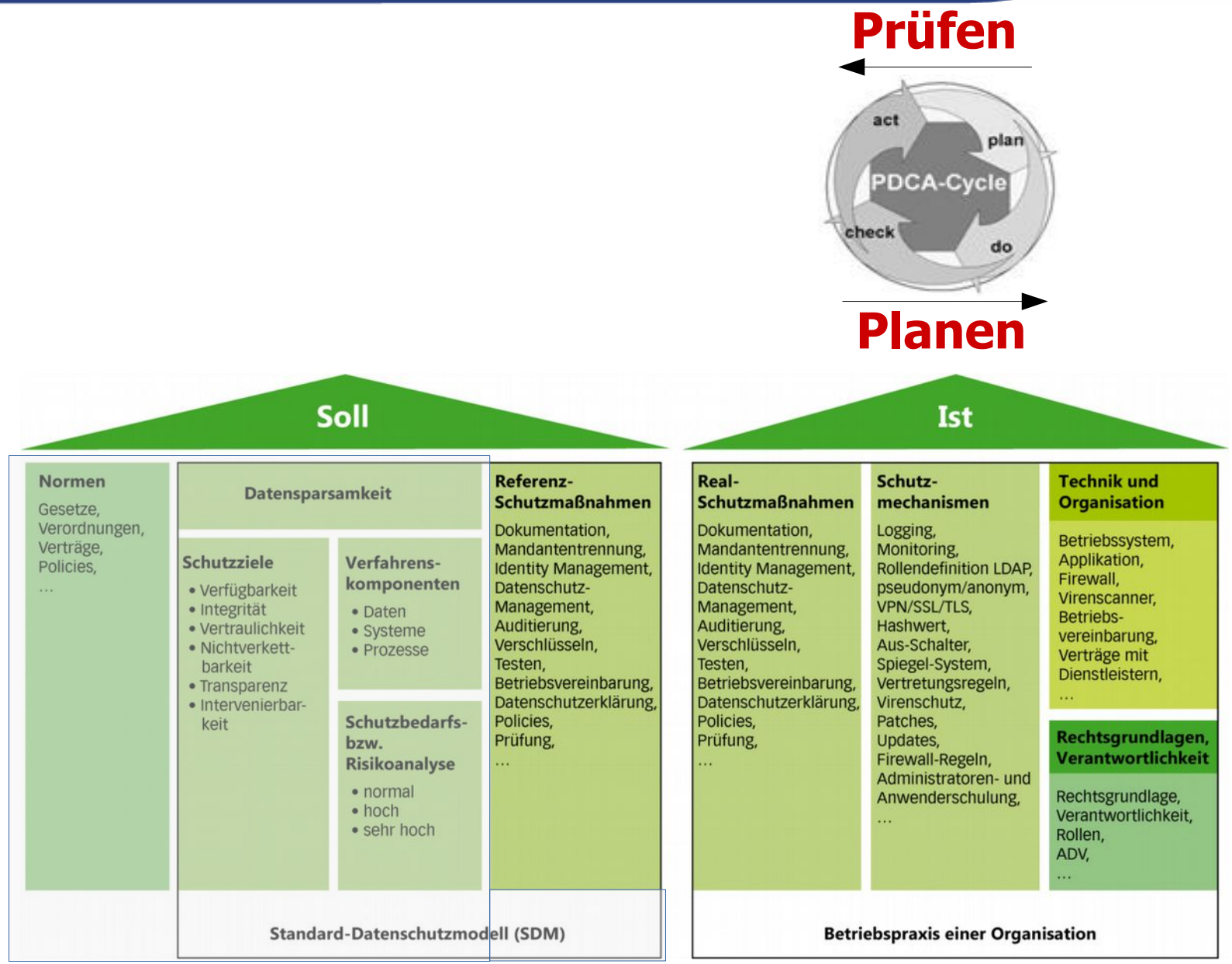
Ein personenbezogenes Verfahren besteht aus drei zu betrachtenden Komponenten:

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

SDM

Das gesamte Modell

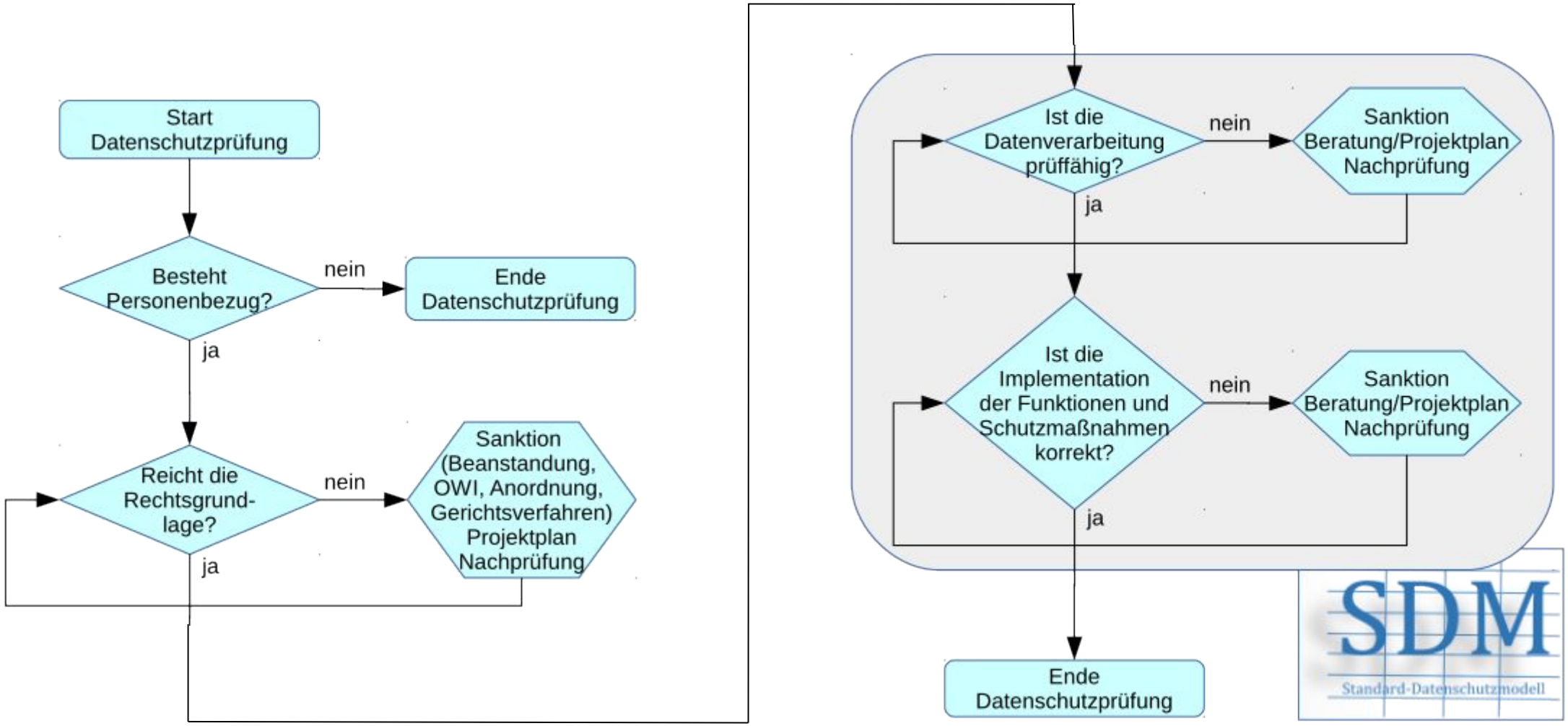
Datenschutz-Management mit SDM



Grafik: M. Rost (ULD)

Standardablauf

einer Datenschutzprüfung, Geltungsanspruch des SDM



Grafik: M. Rost (ULD)

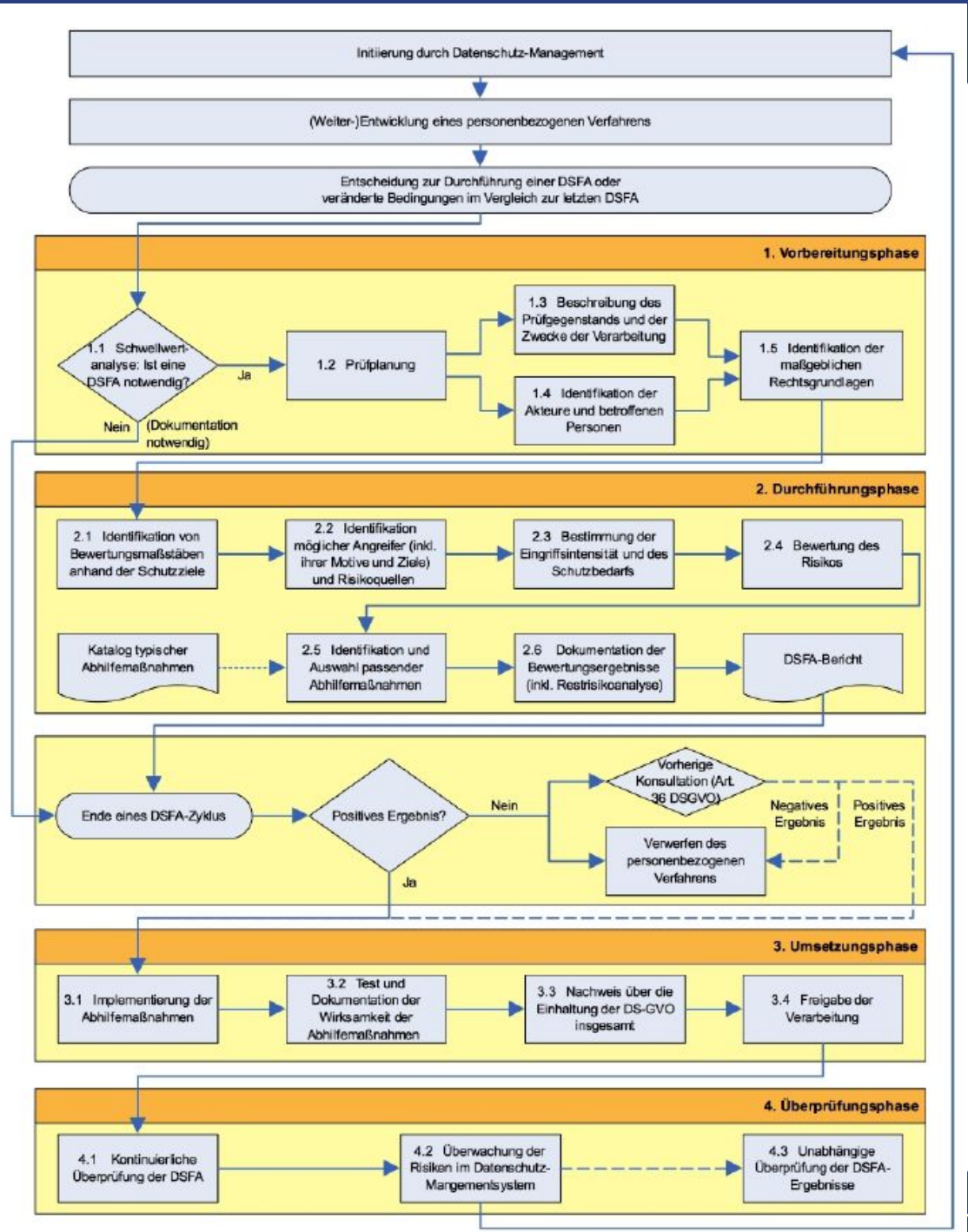
Beispiel für Maßnahmenkatalog für Schulverwaltungs-SW

(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 - rollen- und aufgabenabhängige Gestaltung der Eingabemasken - automatisierte Sperr- und Löschroutinen - Möglichkeit der Anbringung von Sperrkennzeichen - Möglichkeit der Pseudonymisierung nach Bedarf - Möglichkeit der Anonymisierung nach Bedarf - vorkonfigurierbare Exportmöglichkeiten für verschiedene Zwecke (z.B. Informationen für Vereine, etc.) - landesweit abgestimmtes Softwareänderungs-management	- Rechte- und Rollenkonzept - Backup von Daten und Konfiguration nach Backupkonzept - Redundanz der zentralen Systeme - geeignete dezentrale Backupmaßnahmen (z.B. Papierunterlagen oder Backupleitung...) - baulicher Datenschutz (z.B. Brandschutz, Zugangsschutz,...) - Schutz vor Schadsoftware - Firewall - regelmäßige Wartung von Hard- und Software - Vertretungs-regelungen für Personal - Festlegung von Datenformaten - Festlegung der Aufbewahrungsstrategie	- Rechte- und Rollenkonzept - Festlegung der jeweils erforderlichen Erfassungsfrequenz der Datenbestände - Prüfsummen, Hashverfahren - Integritäts-bedingungen für Datenbanken (z.B. Vorgaben für Formate und Wertebereiche) - Integritätsschutz für Software (z.B. Signaturen) - Protokollierungs-verfahren hinsichtlich der Eingabe und Änderung von Daten	- Rechte- und Rollenkonzept - logische Trennung von Schulverwaltungsnetz und Netz für die Lehre - zentrale Administration der verwendeten IT-Systeme durch von der verantwortlichen Stelle Beauftragte - Zugriff auf die Schulverwaltungssoftware nur mit Verfahren nach dem Stand der Technik (u.a. Kryptokonzept, Ende-zu-Ende Verschlüsselung, individualisierte Clientzertifikate, sichere Passwortgestaltung) - baulicher Datenschutz (z.B. Zugangsschutz) - Verpflichtung auf das Datengeheimnis - klare vertragliche Regelungen (z.B. Auftragsdatenverarbeitung, Wartungsverträge) - Mandanten-trennung bei	- Rechte- und Rollenkonzept - Mandanten-trennung bei gemeinsamer Verarbeitung der Daten mehrerer Schulen auf zentralen Datenverarbeitungsanlagen -frühestmögliche Anonymisierung und Pseudonymisierung, - zweckbezogene Pseudonymisierung - Beschränkung der Datenschnittstellen auf das erforderliche Maß - Beschränkung der Funktionalität der Software auf das erforderliche Maß - bei regelmäßiger Übermittlung von Daten an Dritte - ~~durch~~ Bereitstellung eines separaten Abrufdaten-bestandes durch die verantwortliche Stelle	- Rechte- und Rollenkonzept - Möglichkeit der Kenntnisnahme von gespeicherten Daten durch den Betroffenen - Verfahrens-dokumentationen (u.a. Freigabe, Vorabkontrolle, Verfahrensbeschreibung, Sicherheits-konzept, Verträge, Rechtevergabe, relevante Dienst-anweisungen und Dienstvereinbarungen) - Dokumentation von Einwilligungen und Widersprüchen (soweit relevant) - Dokumentation der Softwareversions-verwaltung und anderer Administrations-handlungen - Protokollierungs-verfahren hinsichtlich der Eingabe und Änderung von Daten -Auswertungskonzept für Protokolle - Protokollierung von	- Rechte- und Rollenkonzept - Möglichkeit der Einsicht von Schülern (ggf. Erziehungsberechtigte) in über sie gespeicherte Daten - Möglichkeit des Ausdrucks des über den Betroffenen gespeicherten Daten auf Anforderung (z. B. Schülerstammblatt) - Einrichtung von Prozessen zur Berichtigung, Sperrung oder Löschung von Daten - Rücknahmemöglichkeit von Einwilligungen - Einsichtnahmemöglichkeit in Protokolldateien bspw. zu Übermittlungsvorgängen (ggf. gemeinsam mit dem bDSB) - Verfahren zur Beauskunftung von Datenübermittlungen (ggf. unter Einbeziehung der Empfänger) - 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									

DSFA-Framework



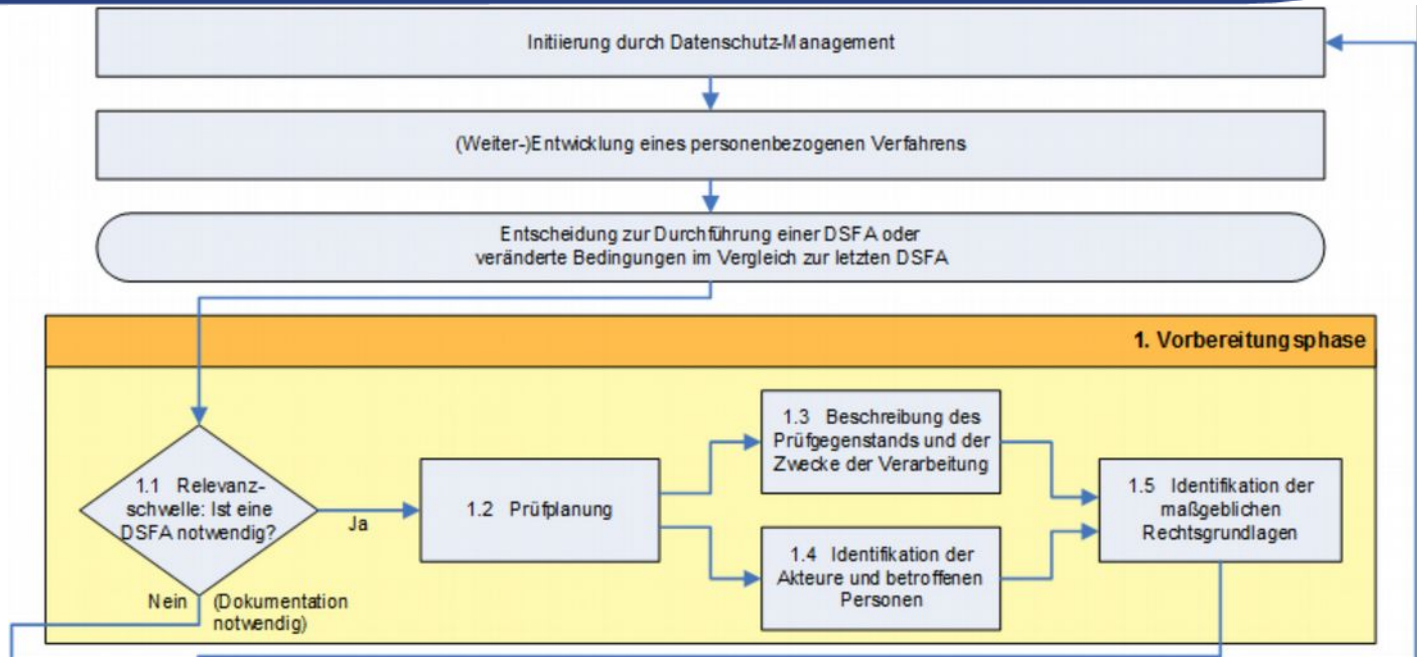
1. Vorbereitung (*Plan*)

2. Durchführung (*Do*)

3. Umsetzung (*Act*)

4. Überprüfung (*Check*)

DSFA-Framework
Phase 1: Vorbereitung



- Das DS-Management, der/die DSB, der/die Verantwortliche stößt DSFA an
- Prüfgegenstand ist eine Datenverarbeitung (**Verarbeitung**):
  Zweckbestimmt, Daten, IT-Systeme, Prozesse, Funktionsrollen
- 1.1 Feststellung der **Relevanzschwelle**
  Muss-Liste der Aufsichtsbehörden, Bestimmen der **Beeinträchtigung** und Abschätzen der **Risiken**
- 1.3 Beschreibung des **ToE** und die **Zwecke der Datenverarbeitung**
- 1.4 Identifikation der beteiligten **Akteure** und **betroffenen Personen**
- 1.5 Identifikation der **Rechtsgrundlagen**

Strategie zur Gewinnung der Risikokriterien: Negation der Grundsätze aus Art. 5!

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**“.

RISIKO (für Betroffene!):

Intransparenz

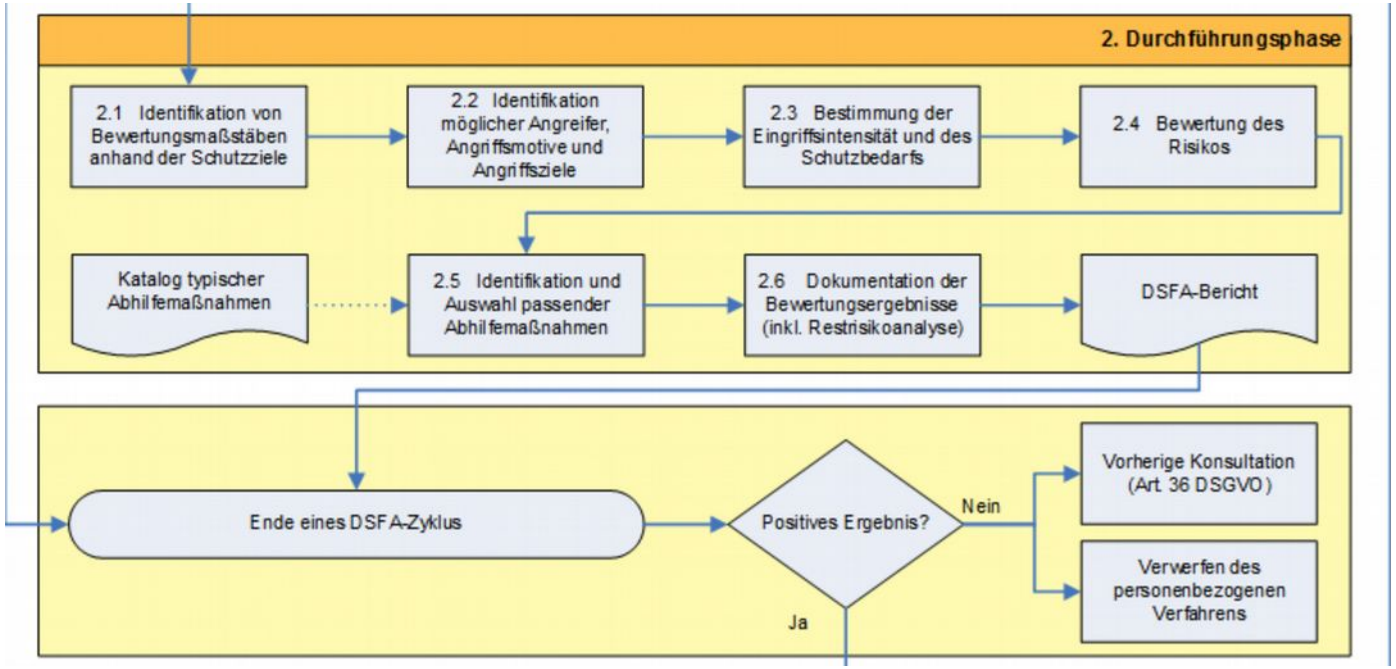
Beliebige Verkettung

Beliebige Datenfülle

Keine Intervenierbarkeit

Mangel an Verfügbarkeit
Mangel an Integrität
Mangel an Vertraulichkeit

DSFA-Framework
Phase 2a: Durchführung



2.1 Bestimmen der **Bewertungsmaßstäbe**
SDM: Gewährleistungsziele

2.2 Bestimmen der **Angreifer**
Ressourcen, Motive, Ziele

2.3 Bestimmen der **Eingriffsintensität** und des **Schutzbedarfs**
SDM: normal, hoch, sehr hoch

2.4 Bewerten des **Risikos**

2.5. Bestimmen **Schutzmaßnahmen**
SDM: Maßnahmenkatalog

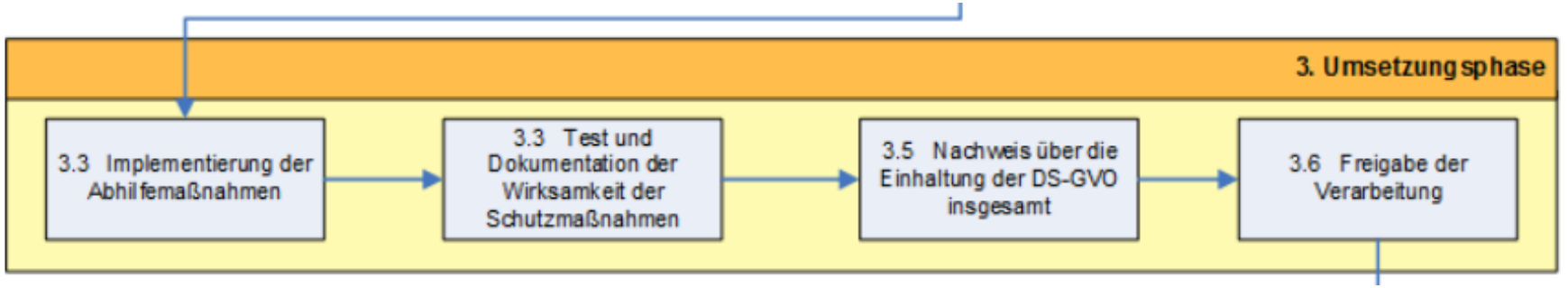
2.6 Dokumentation Bewertungsergebnisse (inkl. **Restrisikoanalyse**)

→ **DSFA-Bericht**

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

DSFA-Framework
Phasen 3: Umsetzung



<u>Umsetzung</u>

3.3 **Implementieren Abhilfemaßnahmen**

SDM-Bausteinekatalog

3.4 **Test und Dokumentation** der Wirksamkeit der Schutzmaßnahmen

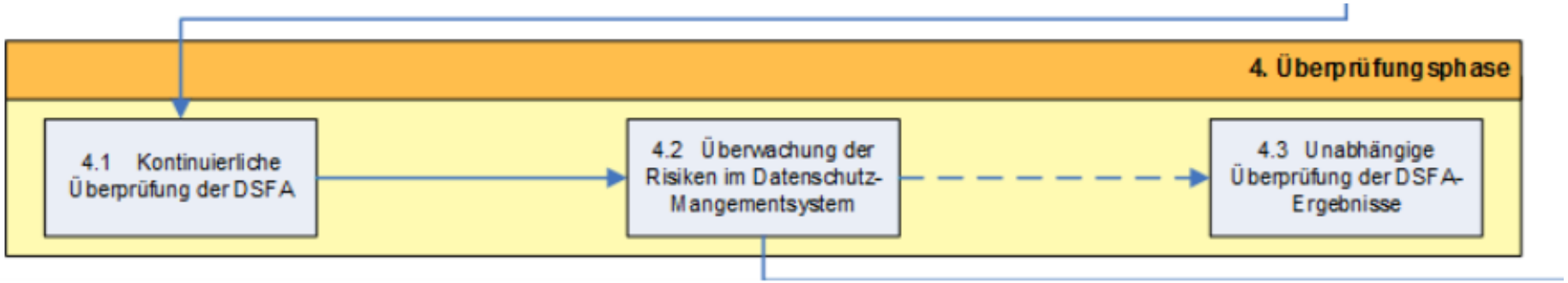
SDM-Maßnahme: Durchführung von Datenschutz-Tests

3.5 Nachweis über **Einhaltung DSGVO** insges.

SDM-Maßnahme: Spezifikation / Dokumentation / Protokollierung

3.6 **Freigabe** der Verarbeitung

DSFA-Framework
Phase 4: Überwachung



Überwachung

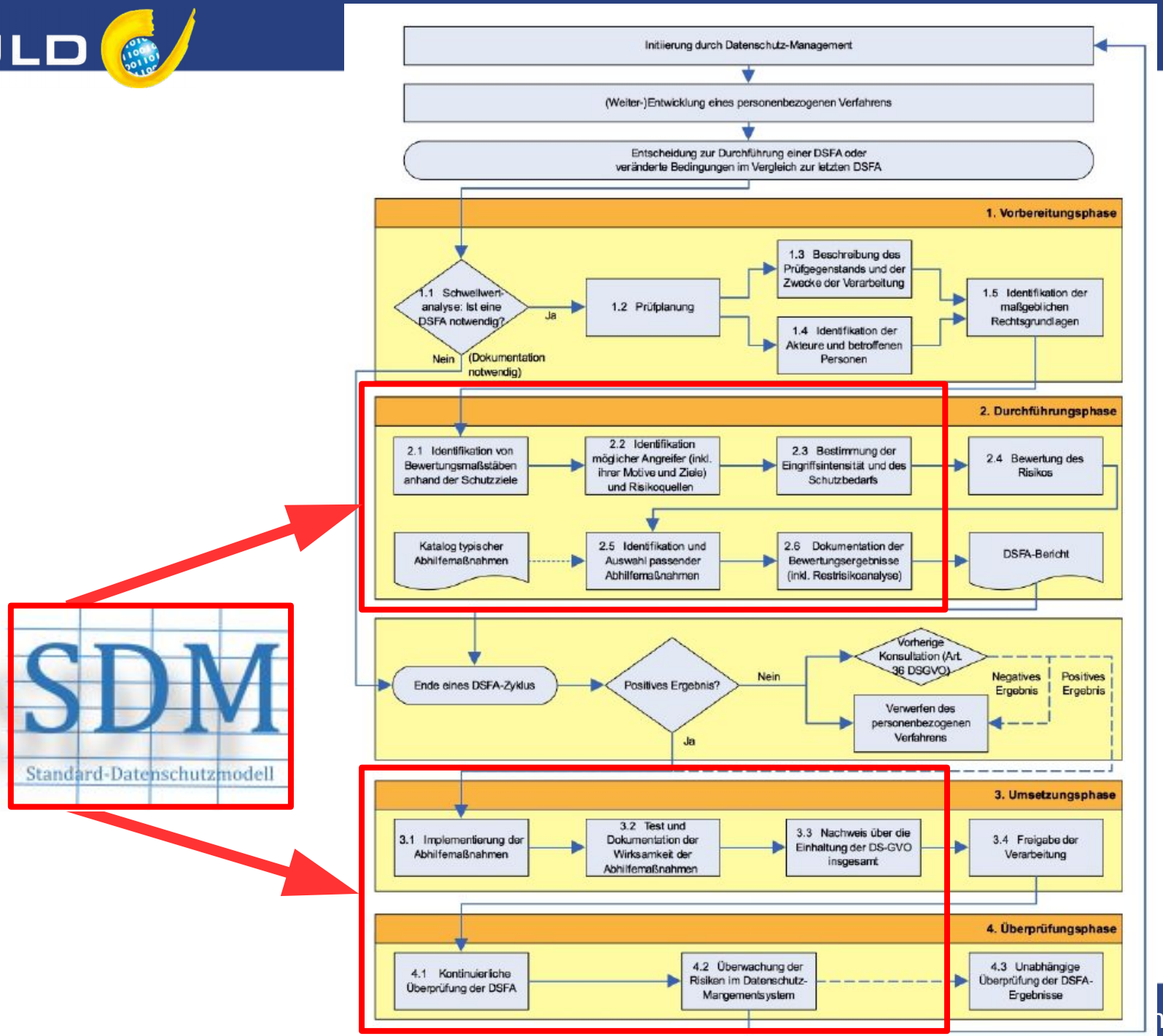
4.1 **Kontinuierliche Überprüfung** der DSFA

Typisches Projektmanagement

4.2 Überwachung der Risiken im **DS-Managementsystem**

Datenschutz-Managementsystem mit SDM

Datenschutz-Folgenabschätzung mit SDM



SDM
Standard-Datenschutzmodell

1. Vorbereitung (*Plan*)

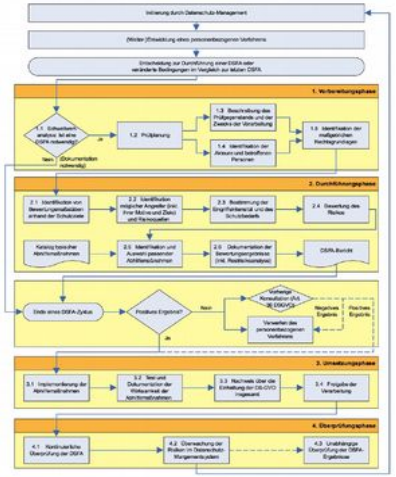
2. Durchführung (*Do*)

3. Umsetzung (*Act*)

4. Überprüfung (*Check*)

Literaturhinweise

DSK: Kurzpapier Nr. 10 – **Risiko für die Rechte und Freiheiten natürlicher Personen**
(Entwurf vom 29.03.2018, Entwurf für DSK-Konferenz am 25.4.2018)



Forum Privatheit: Whitepaper **Datenschutz-Folgenabschätzung, V3.0**
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/