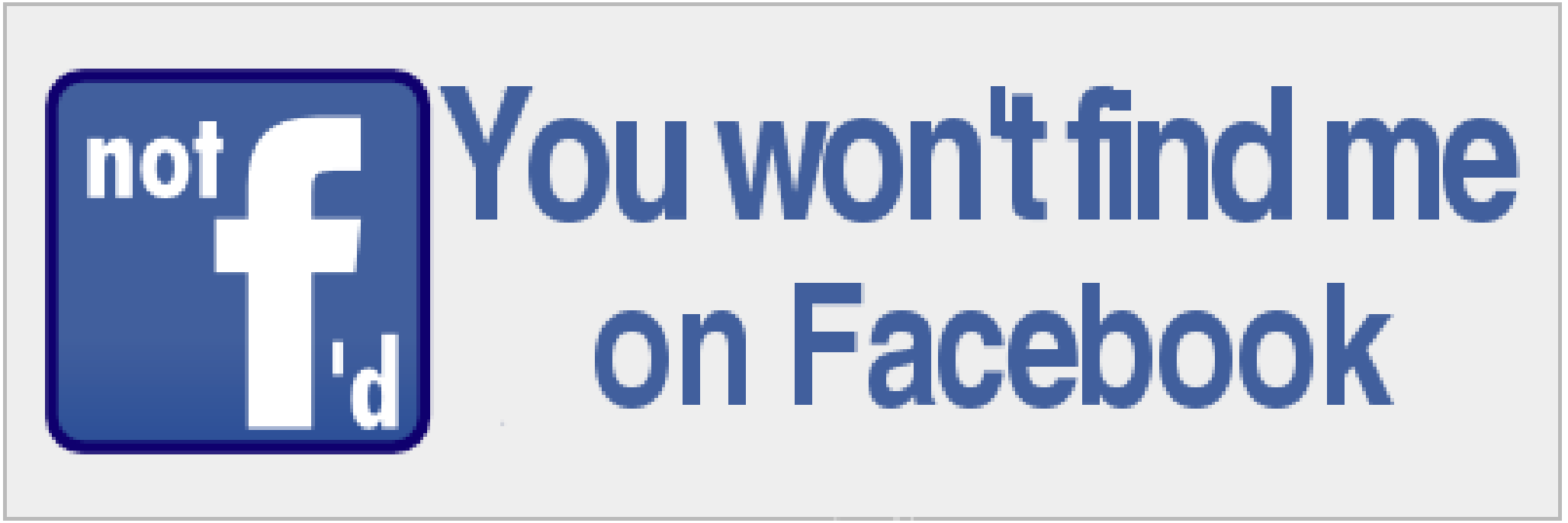
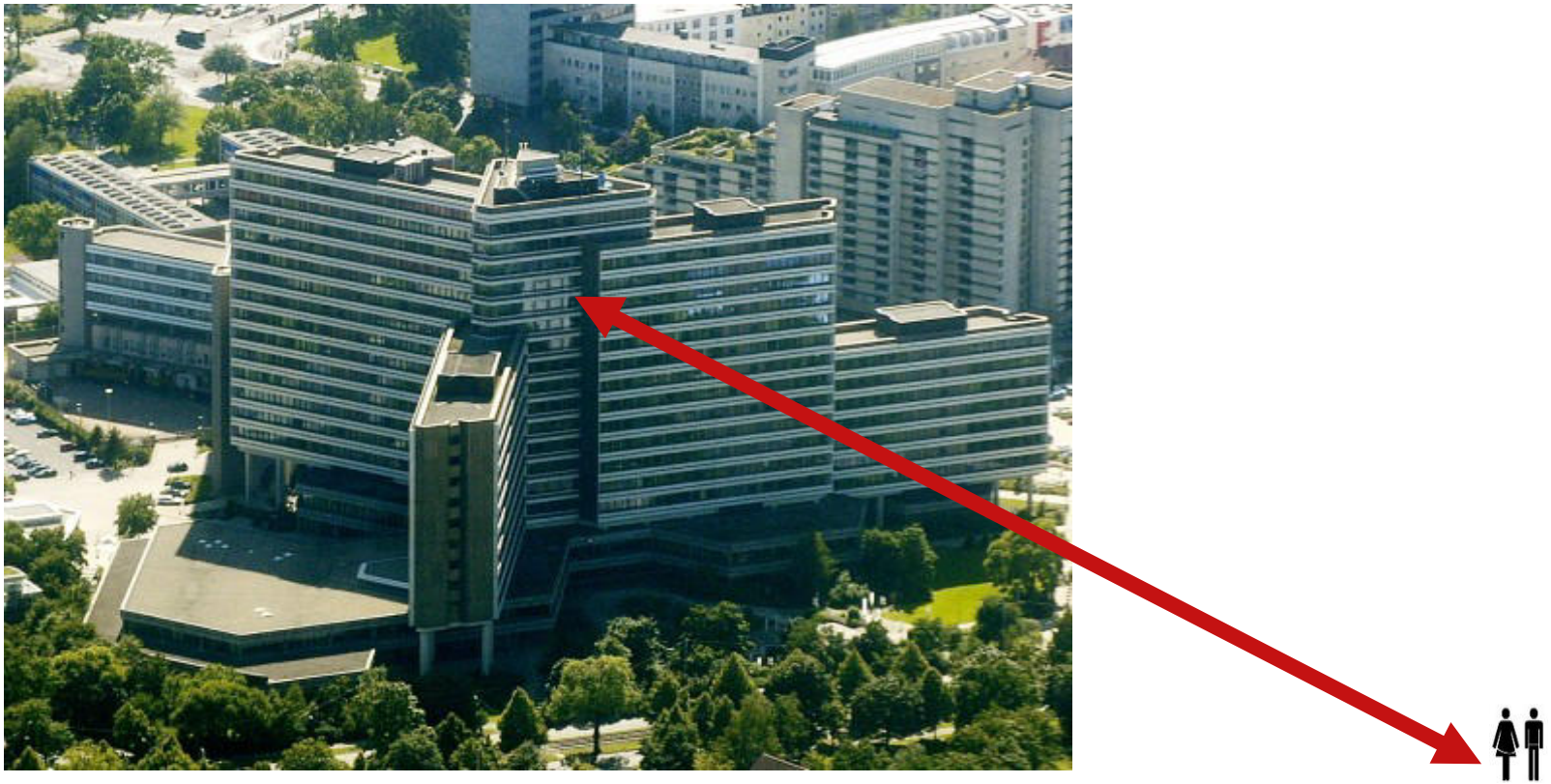
Erfordernisse einer modernen IT und die Herleitung der EU-DSGVO. Das Standard Datenschutz Modell (SDM)

Ron Kneffel (Bredex GmbH)
Ricardo Morte Ferrer(SDM²)

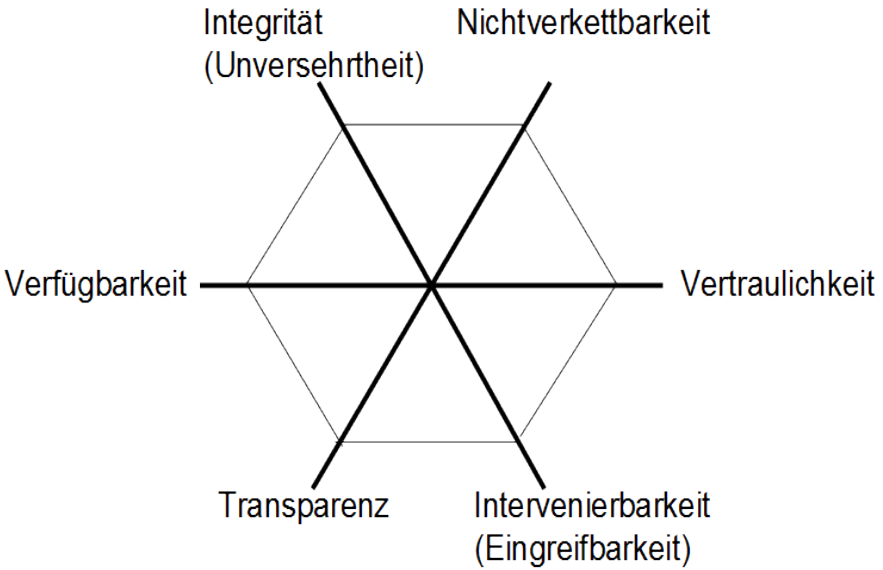
Damit es klar ist



Objektbereich des Datenschutzes



Datenschutz beobachtet, beurteilt und gestaltet die asymmetrischen Machtbeziehungen zwischen mächtigen **Organisationen** (*Risikogeber*) und im Grundsatz selbstständig agierenden **Personen** (*Risikonehmer*).



V

Das Standard-Datenschutzmodell (SDM)

Artikel 32 „Sicherheit der Verarbeitung“

„(…) treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter denderem Folgendes ein:

(…)

*d) ein **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen** zur Gewährleistung der Sicherheit der Verarbeitung.“*

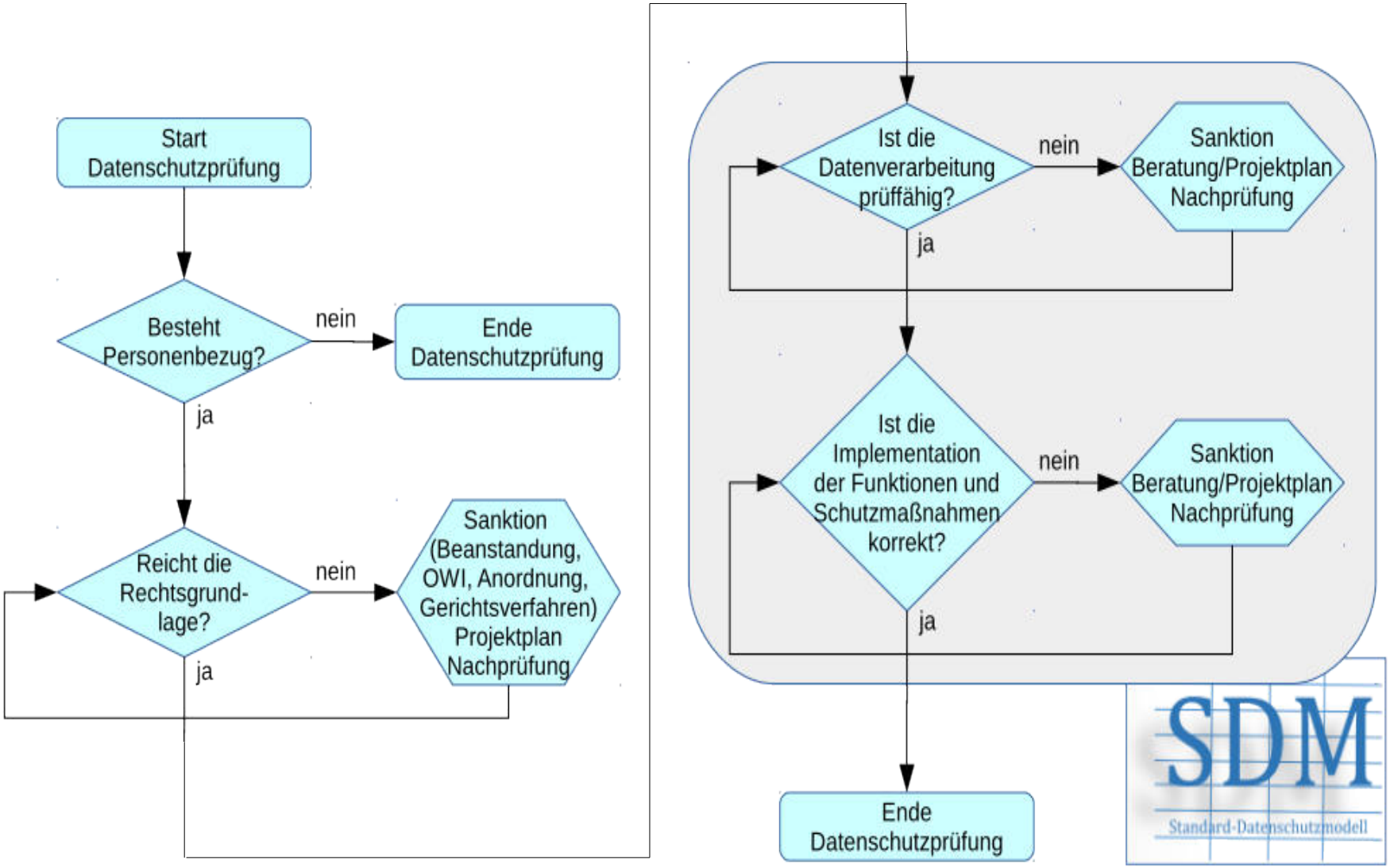
Aktueller Status SDM

V 1.1 - 2018

Das SDM

- ist eine **Methode zur Prüfung und Beratung** des Datenschutzes von Verarbeitungen, zuletzt bestätigt von der DSB-Konferenz 2018/04.
- normativ **verankert in der DSGVO**, methodisch **angelehnt an IT-Grundschutz**
- -Methodik-Handbuch auf **Webseiten** der deutschen Datenschutzaufsichtsbehörden veröffentlicht, es enthält in Kap. 7 eine Auflistung generischer Schutzmaßnahmen.
- in der Version 1.1 wurde gegenüber V1.0 vollständig auf die DSGVO umgestellt.
- umfasst einen **Katalog mit Maßnahmen**, der September 2018 von den Datenschutzbeauftragten der Bundesländer Hessen, Mecklenburg-Vorpommern, Schleswig-Holstein, Sachsen sowie der Evangelischen Kirche Deutschlands veröffentlicht wurde.
- soll **es** mit **Tool-Unterstützung** (bspw. durch Verinice / HiScout) geben. Gespräche mit Toolherstellern laufen.
- liegt für V1.0 in einer Englischversion vor.

Anwendungsbereich des SDM für eine Datenschutzprüfung



Mapping Art. 5 DSGVO und Gewährleistungsziele

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 von Artikeln und Erwägungsgründe (DSGVO) mit Gewährleistungszielen

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, V1.1, S. 21

Typische Maßnahmen zur Umsetzung von Schutzzielen

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

Datenschutz-Risiko

- **<u>Risikotyp 1 „Grundrechtseingriff“:</u> Die Datenverarbeitung einer Organisation ist nicht hinreichend zweckgesteuert**, die Anforderungen der DSGVO werden nicht wirksam umgesetzt.
  - **Risikokriterien?** Negation der Grundsätze des Art. 5 DSGVO (bzw. der Schutzsziele).
  - **Angreifermodell und Szenarien** bestimmen das konkret wirksame operative Risiko: Welche Organisationen haben (auch mit hinreichender Rechtsgrundlage ausgestattet) Interesse an Daten und Ressourcen für einen Zugriff auf die Daten? Der Staat: immer. IT-DL: immer.
  - Organisationen profilieren **die IT-Sicherheitsmaßnahmen nicht nach Datenschutz-Anforderungen.**
- **<u>Risikotyp 2 „Schutzmaßnahmen des Datenschutzes“:</u> Versagen,** bspw. wenn Daten ohne Zweckbindung beliebig verarbeitet werden oder die Protokollierung der Aktivitäten lückenhaft ist oder kein Datenschutz-Controlling implementiert ist.
- **<u>Risikotyp 3 „Schutzmaßnahmen der Informationssicherheit“:</u> Versagen,** bspw. wenn Zugriff durch Unbefugte auf personenbezogene Daten besteht oder deren Korrektheit infrage steht.
- Vielfach wird noch immer nicht verstanden: ISMS muss DSMS folgen!

SDM
das Angreifermodell im Datenschutz

Schutzbedarf haben Personen, er entsteht weil es „Angreifer“ auf Personen gibt. Zur Bestimmung eines Schutzbedarfs ist ein **Angreifermodell** (Motive, Ressourcen, Gelegenheiten) zu formulieren.

Der **Hauptangreifer** zur Bestimmung des Risikos für Grundrechtseingriffe **ist immer die datenverarbeitende Organisation** selbst.

Darüber hinaus gibt es weitere **typische Angreifer**-Organisationen auf Personen:

- Sicherheitsbehörden
- Leistungsverwaltung
- Bereitsteller von IT-(Infrastruktur)Diensten
- Bereitsteller kritischer Infrastrukturen (wie Energieversorger)
- Versicherungen und Banken
- Forschungsinstitute, insbes. psychologischer und sozialwissenschaftlicher Art
- Krankenhäuser, Ärzte, Rechtsanwälte
- Aggressive Startups, Werbeagenturen
- Untätige Aufsichtsbehörden
- Cracker

Risikobestimmung Risikotyp 1 gem. Art. 29-Gruppe

SDM²

1. Bewerten oder Einstufen (Scoring)
   ("Evaluation or scoring")
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
   ("Automated-decision making with legal or similar significant effect")
3. Systematische Überwachung
   ("Systematic monitoring")
4. Vertrauliche oder höchst persönliche Daten
   ("Sensitive data or data of a highly personal nature")
5. Datenverarbeitung in großem Umfang
   ("Data processed on a large scale")
6. Abgleichen oder Zusammenführen von Datensätzen
   ("Matching or combining datasets")
7. Daten zu schutzbedürftigen Betroffenen
   ("Data concerning vulnerable data subjects")
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
   ("Innovative use or applying new technological or organisational solutions")
9. Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert
   ("When the processing in itself prevents data subjects from exercising a right or using a service or a contract")

Wenn aus dieser Liste *zwei Kriterien* zutreffen, besteht für die Freiheiten und Rechte einer Person ein *hohes Risiko* (Risikotyp 1).

Diese **Bestimmung des Riskos** aus der Intensität des Grundrechts- eingriffs bildet die Voraussetzung zur Gestaltung der gesamten Verarbeitung.

aus: WP 248 der Art. 29 Gruppe ab Seite 10 ff.

Verarbeitung
Was ist damit gemeint? (Art. 4 DSGVO)

Begriffsbestimmung *(Artikel 4, Absatz 2: Verarbeitung)*

"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; (….)"

Komponenten von Verarbeitungstätigkeiten

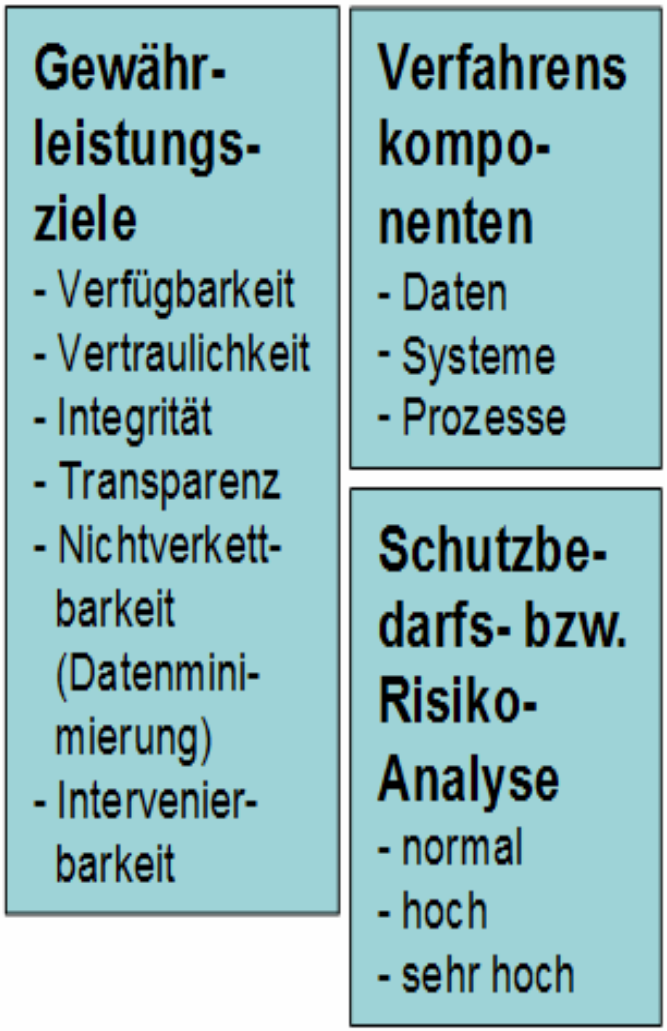
Verarbeitungstätigkeiten nutzen immer drei zu betrachtende Komponenten:

- **Daten**, personenbezogene (mit deren Datenformaten)
- **IT-Systeme** (und Schnittstellen)
- **Prozesse** (und adressierbaren Rollen)

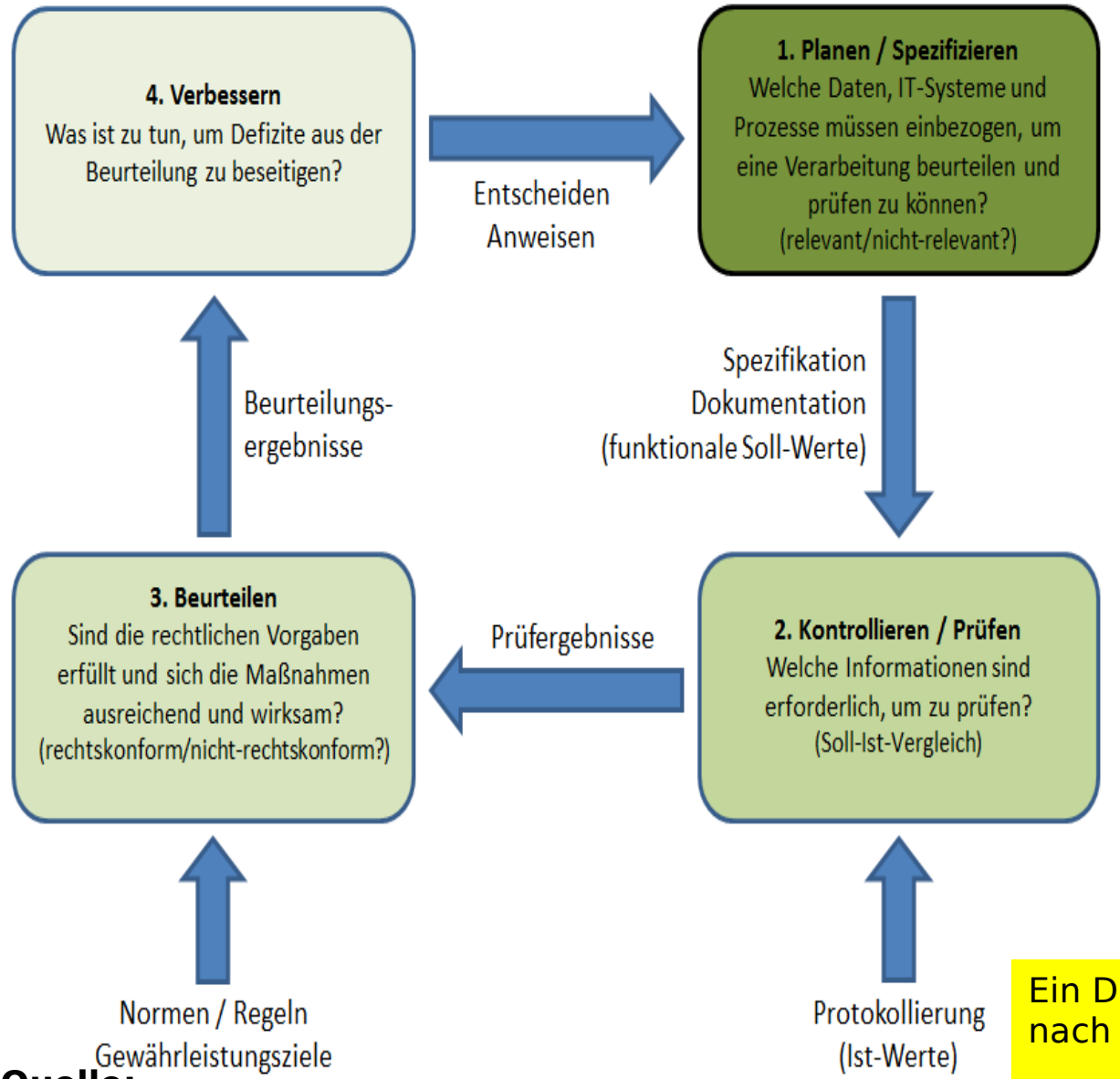
3 Komponenten des Standard-Datenschutzmodells

1. Sechs + 1 Schutzziele, hinterlegt mit einem Maßnahmen-Katalog für jedes Ziel!
2. Drei Schutzbedarfsabstufungen, aus der Betroffenenperspektive formuliert!
3. Drei Komponenten bei Verarbeitungstätigkeiten!

Dies entspricht einem Modell für 7x3x3 (63) (in Wahrheit weniger: 6x3x2 (36) spezifische standardisierte Referenz-Datenschutzmaßnahmen, gegen das sich jede personenbezogene Verarbeitung standardisiert prüfen lässt!



SDM als Framework für Datenschutz-Management gem. Art. 32d DSGVO



1. Schutzmaßnahmen für relevante Verarbeitungskomponenten bestimmen und deren Prüffähigkeit spezifizieren. (*Plan*)

2. Prüfergebnisse anhand funktionaler Soll-Ist-Differenzen herstellen, die rechtlich beurteilt werden können. (*Do*)

3. Rechtliche Beurteilung von Prüfergebnissen erzeugen. (*Check*)

4. Aus rechtlichen Beurteilungen der Verarbeitung Veränderungsbedarfe formulieren und deren Umsetzung initiieren. (*Act*)

Ein DSMS unterliegt seinerseits der Anforderung nach kontinuierlicher Verbesserung.

Quelle:
Baustein „Datenschutz-Management“

SDM, V1.1 Aktuelle Bausteine (Stand: 2018-0910)

SDM

Maßnahmenkatalog

Der Maßnahmenkatalog zum SDM befindet sich noch in der Erarbeitungsphase. Die einzelnen Bausteine des Katalogs werden sukzessive veröffentlicht und zur Anwendung freigegeben.

Wir weisen ausdrücklich darauf hin, dass die hier veröffentlichten Bausteine noch nicht in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder abgestimmt worden sind. Wir empfehlen den Anwendern, ihre Erfahrungen bei der Erprobung der Bausteine den an der Entwicklung der Bausteine beteiligten Datenschutzbehörden mitzuteilen, und somit zur Weiterentwicklung von Methode und Maßnahmen beizutragen.

Bezeichnung	Format	Größe
Baustein 11 „Aufbewahrung“	PDF	0.52 MB
Baustein 41 „Planung und Spezifikation“	PDF	0.63 MB
Baustein 42 „Dokumentation“	PDF	0.61 MB
Baustein 43 „Protokollierung“	PDF	0.53 MB
Baustein 50 „Trennung“	PDF	0.63 MB
Baustein 60 „Löschen und Vernichten“	PDF	0.61 MB
Baustein 80 „Datenschutzmanagement“	PDF	0.84 MB

Newsletter

- **Löschen**
- **Aufbewahrung**
- **Protokollierung**
- **Dokumentation**
- **Planung / Spezifikation**
- **Trennung**
- **Datenschutzmanagement**

https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

SDM-Bausteine in der Warteschlange

(Stand: 2018/0910)

10 Verfügbarkeit

Baustein „Aufbewahrung“
Baustein „***Datensicherung und -wiederherstellung***“

20 Integrität

30 Vertraulichkeit

40 Transparenz

Baustein „Planung und Spezifikation“
Baustein „Dokumentation“
Baustein „Protokollierung"
Baustein „***Auskunft***“

50 Nichtverkettbarkeit

Baustein „Trennung“
Baustein „***Rollen und Berechtigungen***“
Baustein „***Anonymisierung & Pseudonymisierung“***

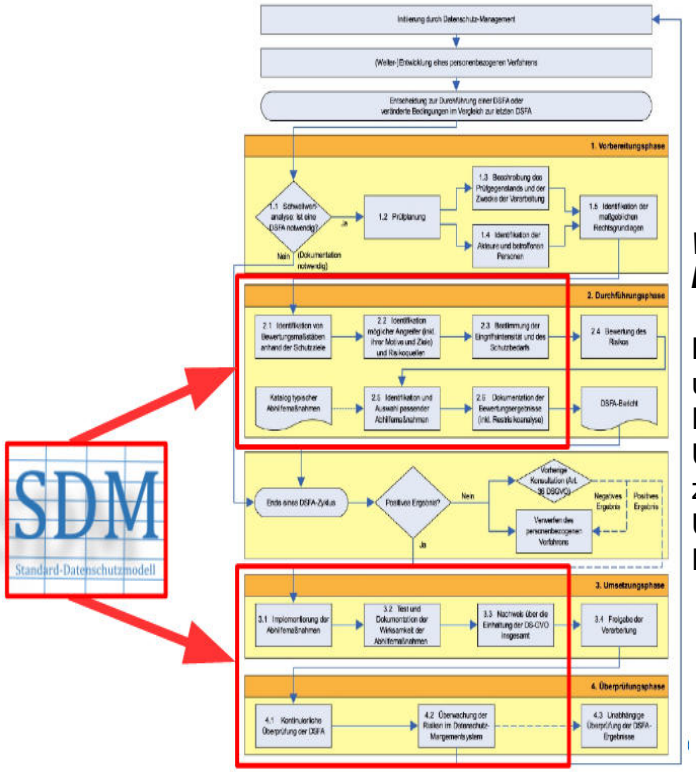
60 Intervention

Baustein „Löschen“
Baustein „***Berichtigung***“
Baustein „***Sperren***“

80 Datenschutz-Framework

Baustein „Datenschutz-Management“

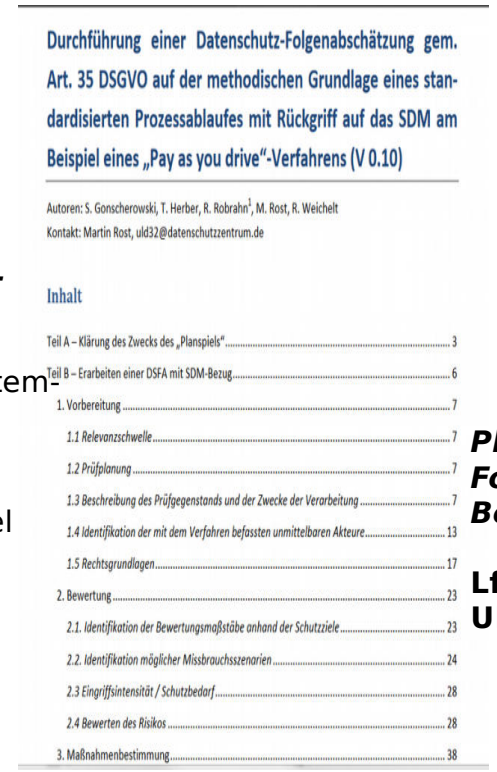
Datenschutz-Folgenabschätzung (nach Art. 35 DSGVO) mit SDM



Whitepaper „Datenschutz-Folgenabschätzung“

Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe
ULD (Unabhängiges Landes-zentrum für Datenschutz), Kiel
Universität Kassel, Institut für Wirtschaftsrecht

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



Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO auf der methodischen Grundlage eines standardisierten Prozessablaufes mit Rückgriff auf das SDM am Beispiel eines „Pay as you drive“-Verfahrens (V 0.10)

Autoren: S. Gonscherowski, T. Herber, R. Robrahn, M. Rost, R. Weichelt
Kontakt: Martin Rost, uld32@datenschutzzentrum.de

Inhalt

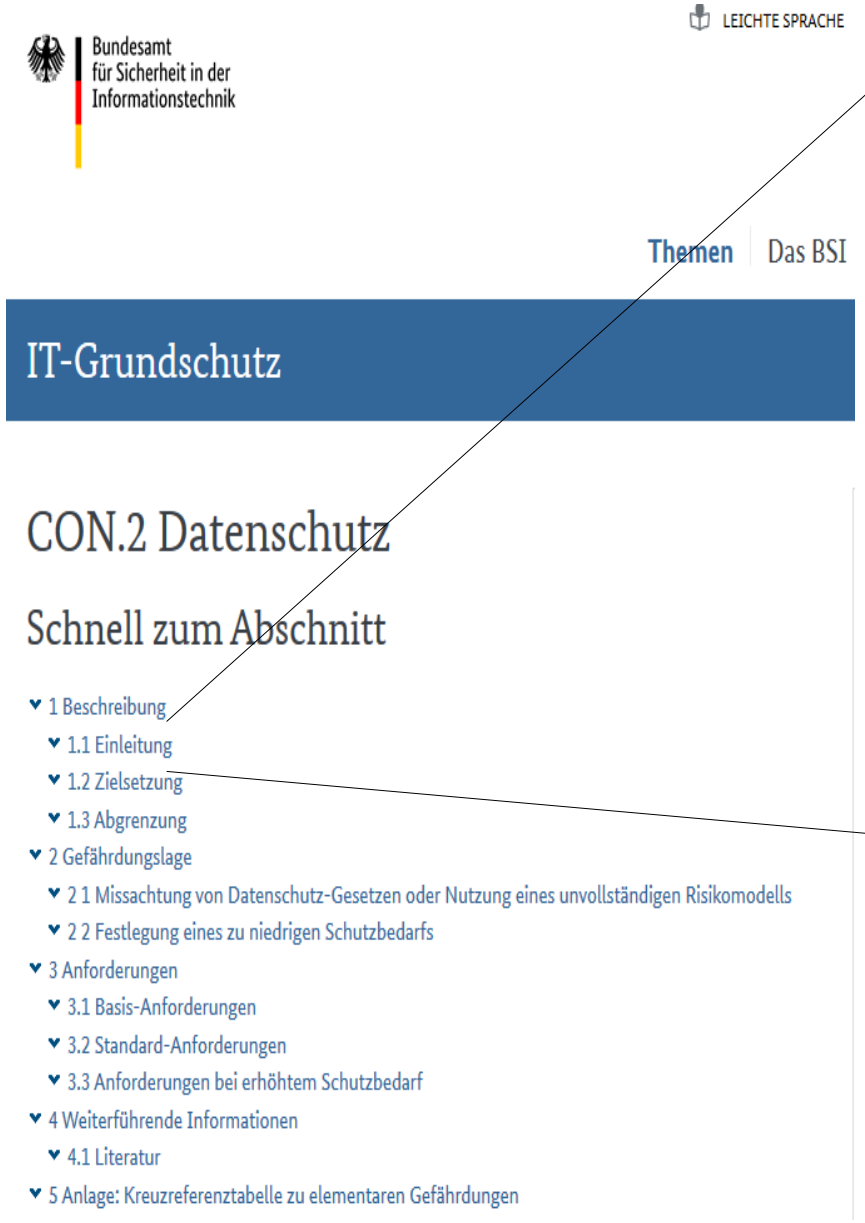
Teil A – Klärung des Zwecks des „Planspiels“ ... 3
Teil B – Erarbeiten einer DSFA mit SDM-Bezug ... 6
1. Vorbereitung ... 7
1.1 Relevanzschwelle ... 7
1.2 Prüfplanung ... 7
1.3 Beschreibung des Prüfgegenstands und der Zwecke der Verarbeitung ... 7
1.4 Identifikation der mit dem Verfahren befassten unmittelbaren Akteure ... 13
1.5 Rechtsgrundlagen ... 17
2. Bewertung ... 23
2.1. Identifikation der Bewertungsmaßstäbe anhand der Schutzziele ... 23
2.2. Identifikation möglicher Missbrauchsszenarien ... 24
2.3 Eingriffsintensität / Schutzbedarf ... 28
2.4 Bewerten des Risikos ... 28
3. Maßnahmenbestimmung ... 38

Planspiel „Datenschutz-Folgenabschätzung“ am Beispiel „pay-as-you-drive“

LfD-Mecklenburg-Vorpommern
ULD Kiel

https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf

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

Fragen?

Sie dürfen auch nach der Veranstaltung gern Kontakt zu mir aufnehmen.

SDM²

Telefon, 0172/4151086
https://sdm2.de/

rmorte@sdm2.de