Standard-Datenschutzmodell

Praktische Anwendung des SDM-Würfels im Rahmen einer Datenschutz-Folgenabschätzung

Sommerakademie
am 11. September
2023 in Kiel

Karin de Lange
Tel.: 04531 160 1583
k.delange@kreis-stormarn.de
Mommsenstraße 13, 23843 Bad Oldesloe

Martin Rost
Tel.: 0431 988-1391
ULD32@datenschutzzentrum.de
https://www.datenschutzzentrum.de/

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Agenda

1. Neues vom SDM-V3
   - Der „Würfel“
   - Was meint „SDM-Konformität“?
2. SDM-Tools
   - Vorschläge zur Typisierung
3. Verschiedenes
   - Gründung SDM-Usergroup
   - Hinweis auf das SDM-Buch
   - Ausblick auf kommende Arbeiten am SDM
4. DSFA mit SDM
   - Anwendung des SDM-Würfels in der Praxis
     -> Frau de Lange

Zur Erinnerung: Was leistet das SDM?

Mit Hilfe des Standard-Datenschutzmodells (SDM) können die **normativen Anforderungen** des Datenschutzrechts, also insbesondere Anforderungen der DSGVO, an *personenbezogene Verarbeitungen* (Geschäftsprozesse, Verfahren) in Organisationen in **funktionale Anforderungen** (Aufgaben, Technik) transformiert werden.

Aktueller Status SDM

Das SDM-V3...

- wurde von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder Deutschlands (DSK) im **November 2022** zum dritten Mal bestätigt bzw. angenommen.
- hat **neue Inhalte** gegenüber SDM-V2:
  - Übereinstimmende **Definition von Risikotypen** mit IT-Grundschutz des BSI
  - Modellierungsvorgabe einer personenbezogenen Verarbeitung in drei Dimensionen („**SDM-Würfel**“):
    - 9 **Vorgängen** oder 4 **Phasen** (Erhebung, Organisation, Nutzung, Löschung) sowie
    - 3 Ebenen (Verfahrenslogik, Sachbearbeitung, AV) müssen anhand der
    - 7 Gewährleistungsziele analysiert, mit risikomindernden Maßnahmen versehen werden, worüber der Nachweis gem. Art. 5 DSGVO zu erbringen ist.
- liegt in **Englischübersetzung** vor.

Zentrales **Repository:** https://www.datenschutz-mv.de/datenschutz/datenschutzmodell

1 Neues zum SDM

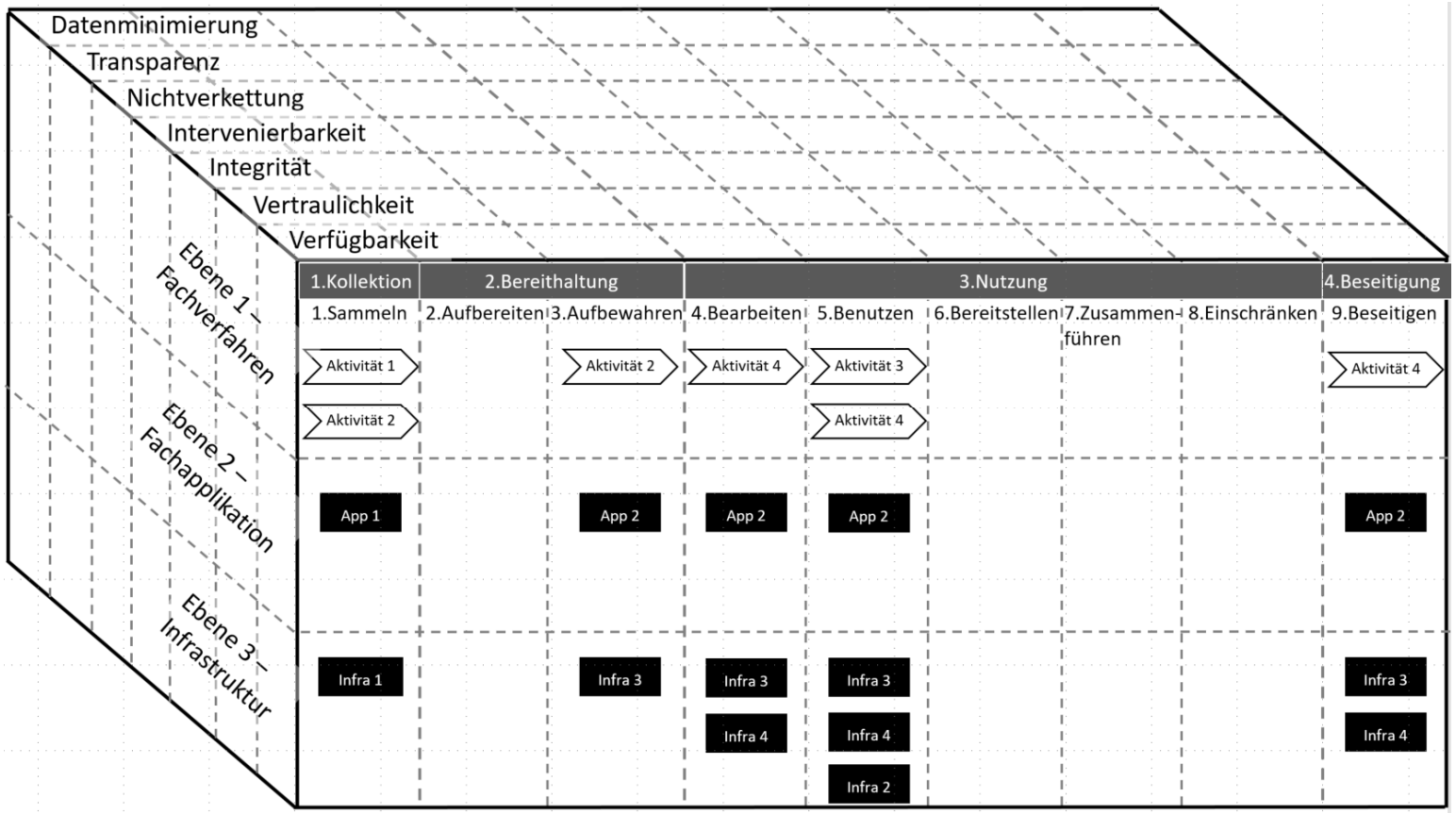
Definition der Risikotypen in SDM-V3

- Risikotyp A
  Der Grundrechtseingriff bei natürlichen Personen durch die Verarbeitung ist **nicht hinreichend milde** gestaltet.
- Risikotyp B
  Die Maßnahmen zur Verringerung der Eingriffsintensität einer Verarbeitung sind, in Bezug auf die Gewährleistungsziele, **nicht vollständig oder werden nicht hinreichend wirksam betrieben oder nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.**
- Risikotyp C
  Die Maßnahmen, die nach der **Informationssicherheit** geboten sind (vgl. z. B. IT-Grundschutz nach BSI), sind nicht vollständig oder werden nicht hinreichend wirksam betrieben oder werden nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.
- Risikotyp D
  Die **Maßnahme der Informationssicherheit werden nicht ausreichend datenschutzgerecht**, im Sinne des Risikotyp A und Risikotyp B, betrieben.

(Diese Definition der Risikotypen ist wortgleich zum IT-GS/CON.2 (BSI 2023: IT-Grundschutz-Bausteine, Edition 2023, "CON.2 Datenschutz“)

1 Neues zum SDM

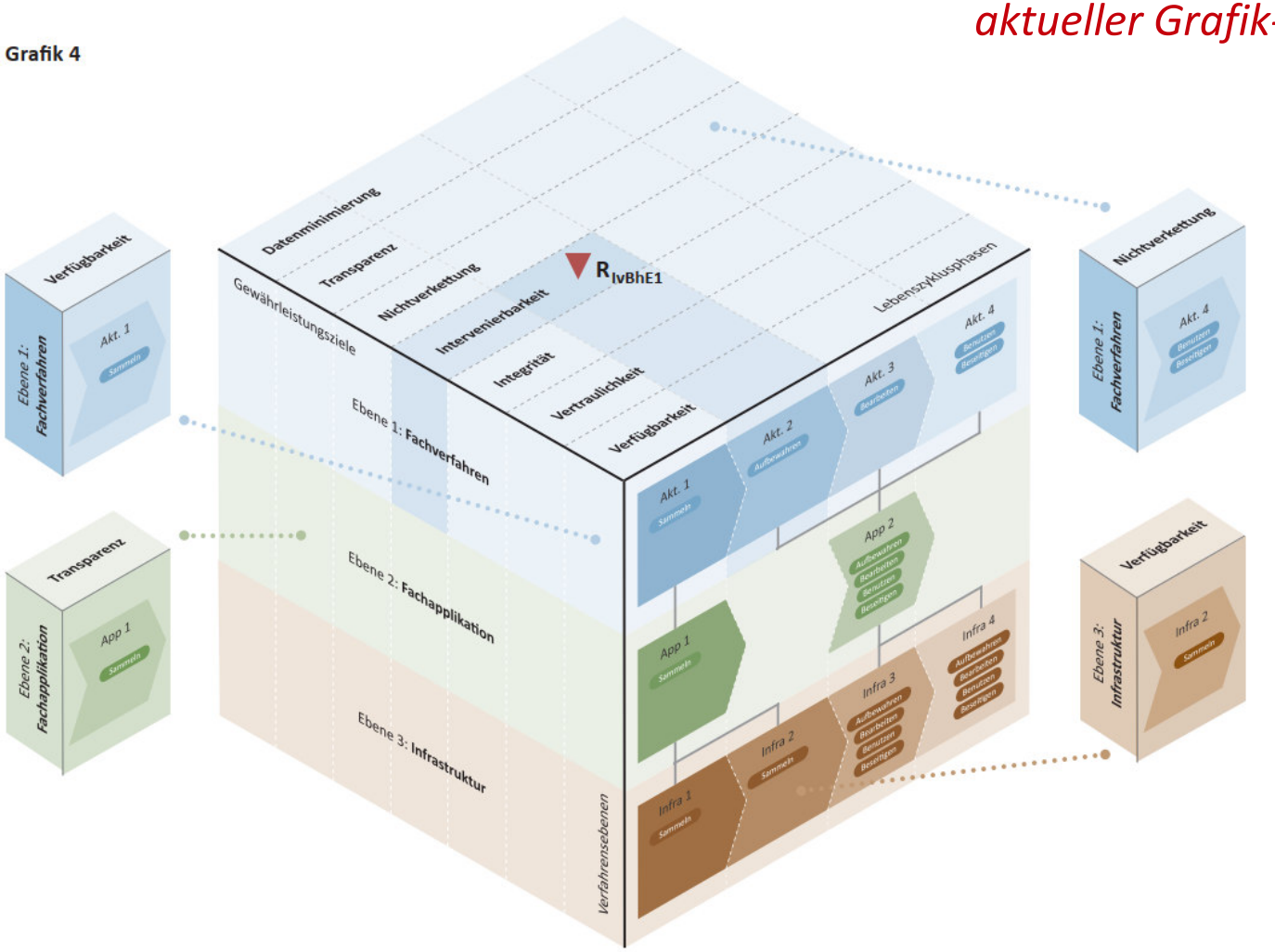
SDM-Würfel



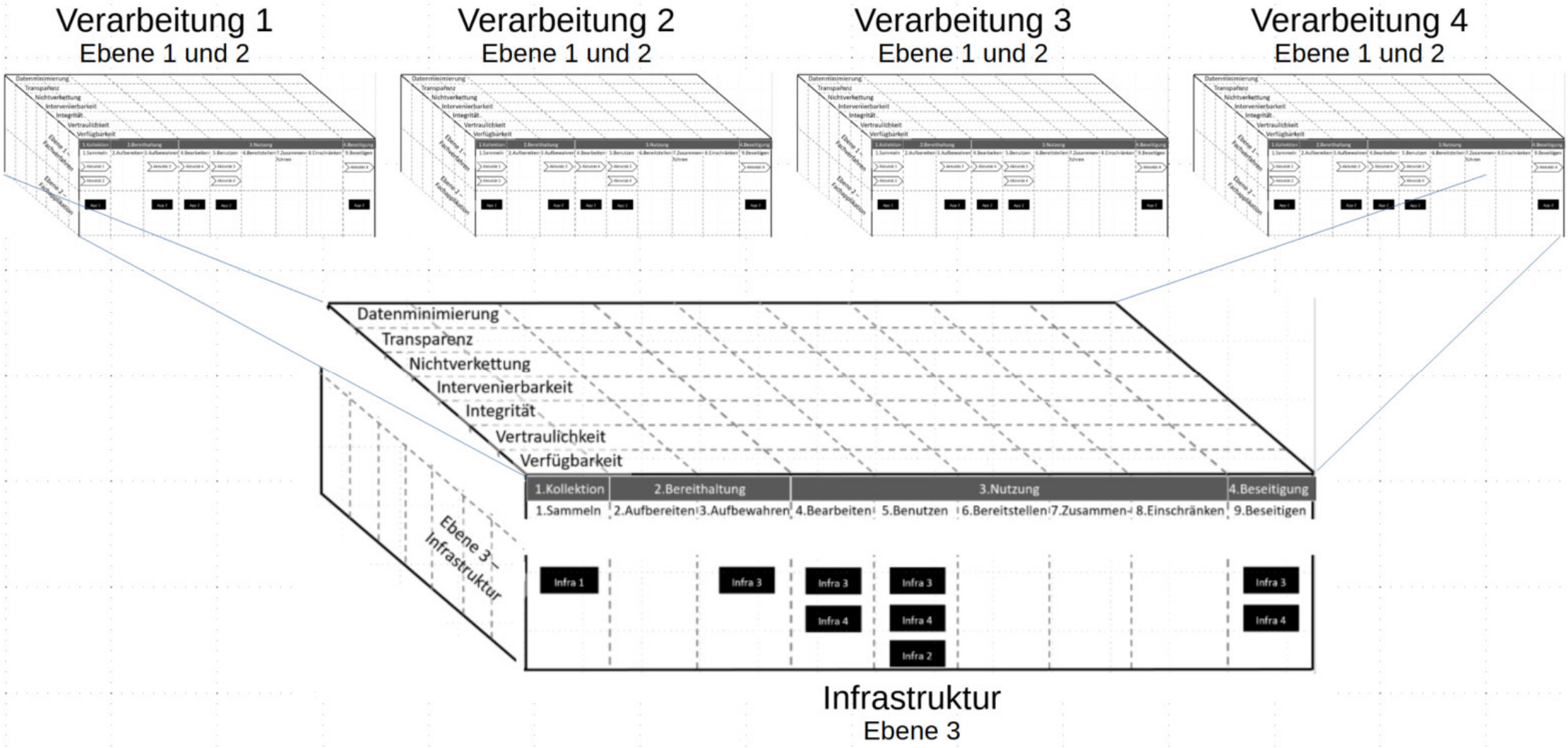
Der SDM-Würfel

aktueller Grafik-Entwurf (10.07.2023)

Grafik 4



Der SDM-Würfel



Was heißt „SDM-Konformität“?

SDM-Konformität liegt vor, wenn Datenschutzaktivitäten ...

- an der **Gestaltung einer Verarbeitung** personenbezogener Daten ansetzen (s. Art. 4 Nr. 2 DS-GVO) und eine Verarbeitung in einzelne a) **Verarbeitungsvorgänge bzw. Phasen** sowie in b) **drei Ebenen**, c) jeweils mit **Daten, IT-Systemen und Prozessen** unterteilt wird (also nicht nur der „besondere Schutz personenbezogener Daten“ in den Blick genommen wird);
- als Risikokriterien das vollständige Set der „**Gewährleistungsziele**“ in Bezug auf die Verarbeitungsvorgänge genutzt wird (und nicht die Risiken der IT-Komponenten oder die drei Schutzziele der IT-Sicherheit den Ausgangspunkt bilden);
- die Datenschutzrisiken für Personen entlang der **Intensität des Grundrechtseingriffs** einer Verarbeitung durch eine Organisation (s. Art. 8 der EU-GrCh) beurteilt werden (und diese nicht mit den Haftungsrisiken der Organisation oder Risiken der Informationssicherheit verwechselt werden);
- zu jedem Grundsatz der DSGVO bzw. jedem Gewährleistungsziel Bezug auf die **Referenzschutzmaßnahmen** zur Risikominderung hergestellt wird (also nicht formal bzw. pauschal jede Maßnahme aus den SDM-Bausteinen „auf grün gesetzt“ wird);
- vom Datenschutzrecht ausgehen und funktionale Prüfungsergebnisse dem **Letzturteil aus dem Datenschutzrecht** unterworfen werden.

2 Sichtung von SDM-Unterstützungsprogrammen

- **12 Tool-Entwickler** stellten nach einem Aufruf im SDM-Newsletter und SDM-Forum des BfDI ihre SDM-Tools am 6./7.12.2022 der UAGSDM vor.
  - Voraussetzung zur Teilnahme war die Beachtung des 4-seitigen Papiers „**Anforderungskatalogs an ein SDM-Tool**“. Im Nachgang wurde um die Beantwortung eines Fragebogens gebeten.
- Das Ergebnis:

Note	Bedeutung	Anzahl der Tools („+“, wenn Entwicklungsbereitschaft seitens des Herstellers erkennbar)	Typische Tool-Form
A	Inhalt, Methode und Programm gut	1 (A+)	Modellierungs-DB („Mockup“)
B	Inhalt und Methodisch gut, Programmschwächen	3 (2 x B+)	Tabellenkalkulation
C	inhaltliche und methodische Schwächen, Programm gut	3 (2 x C+)	Modellierungs-DB
D	weder inhaltlich noch methodisch noch Programm gut	4	
E	unklar	1	

2 Sichtung Tools Produktnamen

- audatis MANAGER**
- Caralegal**
- Compliance Aspekte
- DARAS (Documentation and Risk Assessment Standardized)**
- Datenschutz für Kleine
- Datenschutz-Tool (moewe)**
- DS-GVO Audit nach dem Standard-Datenschutzmodell (SDM) 2.0 (datakontext)
- ECOMPLY Datenschutz-Management-Software**
- HiScout GRC Suite
- Privacy Pilot 2.0 (Scheja-Partner)**
- SDM-Tool (Scheja-Partner)**
- Verinice

** Diese Hersteller nahmen im Januar 2023 an einer zweitägigen SDM-Schulung teil. Die Schulung führt bei allen teilnehmenden Herstellern dazu, Veränderungen an ihren Tools durchzuführen. Eine erneute Sichtung dieser überarbeiteten Tools durch die UAGSDM steht noch aus.

2 Sichtung Tools Eigenschaften

- Verwendung von SDM-Modellierungskomponenten
  - Verarbeitungsorientierung
  - Gewährleistungsziele zur Risikobestimmung
  - Auf Gewährleistungsziele abgestimmte Schutzmaßnahmen
- Methodische Führung
  - Keine Führung durch das Programm (verlangt Expert*innenwissen) oder Erzwingungen des methodischen Vorgehens durch Programmablauf („Wizard-Modus“)
- Output
  - Nachweise (gem. DSGVO)
  - Prüfberichte (Audit gem. DSGVO/ SDM)
  - Anweisung (bspw. zur schrittweisen Durchführung DSFA)
  - DS-Konzept (Erstellung Schutzmaßnahmen, Etablieren DS-Management (DSM))
  - Anweisungen bzgl. DSM (Controllen (Erkennen, Regeln/Steuern) von Schutzmaßnahmen (Dashboard, (Teil-)Automatisierung (Buzzword: "Datenschutz-Prüf-KI"))
  - ...
- Tooltyp
  - Universaltool: Deckt alle Anforderungen der DSGVO ab
  - Fokustool: Deckt Teile der Anforderungen der DSGVO ab (typ: DSFA, Maßnahmen-Audit)
  - Expertentool: Erzeugt Leitfäden für Prüfungen, DSFA, DSM, Audit etc.
  - Enterprise-Betrieb: Ist organisationsweit installiert (inkl. Filialen/Nebenstellen), verlangt aufwändige Installation

2 Sichtung Tools
Vorschläge zur Kennzeichnung

- SDM-VE: Nutzt die Unterscheidung der drei Verfahrensebenen
- SDM-DSP: Nutzt die Unterscheidung Daten, Systeme, Prozesse
- SDM-VV: Nutzt die Unterscheidung der neun Verarbeitungsvorgänge
- SDM-VP: Nutzt die Unterscheidung der vier Verarbeitungsphasen
- SDM-GZ: Nutzt das vollständige Set der Gewährleistungsziele
- SDM-GR: Nutzt die grundrechtsorientierte Risikomodellierung anhand der Gewährleistungsziele (maßgeblich ist Bestimmung der Eingriffsintensität, nicht „möglicher Schaden“)
- SDM-GM: Nutzt den vollständigen Katalog generischer Maßnahmen
- SDM-BS: Nutzt den vollständigen Katalog veröffentlichter SDM-Bausteine
- SDM*: Das Tool nutzt das vollständige Set der SDM-Komponenten

3 Verschiedenes
Gründung SDM-Usergroup

- Im Oktober ist die Gründung einer **SDM-Usergroup** vorgesehen.
- Aktuelle Probleme der Weiterentwicklung des SDM:
  - zu **geringe Produktivität** der UAGSDM (zu wenige Autor*innen) bzgl. Baustein-Entwicklung
  - **Überarbeitung** der Maßnahmen notwendig (bessere Abstimmung der Maßnahmen mit den neuesten Modell-Entwicklungen, bspw. der Bezug zum Würfel)
  - Die große **Mitarbeitsbereitschaft insbesondere an Bausteinen** außerhalb der UAGSDM, bspw. durch erfahrene SDM-Nutzer, wird nicht genutzt
  - Bislang wurde **kein Kanon bzgl. der Ausbildung zur Anwendung des SDM** ausgebildet, viele schlechte SDM-Schulungsangebote
  - keine (auch nur begleitende) Entwicklung von **SDM-Tools** durch DS-Aufsichtsbehörden…
- Ziel der SDM-UG u.a.:
  - Institutionalisierung der Verbindung zwischen **DS-Aufsichtsbehörden/UAGSDM und der SDM-Anwendungs- und Entwicklungspraxis**
  - Entwicklung und Durchführung von **qualitätsgesicherten SDM-Schulungen** und **Zertifizierungen**
  - Pool für kompetente **DSFA-Projektmanager*innen**, **Tool-Entwickler*innen**, **DS-Auditor*innen**
  - Plattform für den **Austausch unter SDM-Anwender*innen**
  - …

3 Verschiedenes
SDM-Buch

Rost

Das Standard-Datenschutzmodell (SDM)

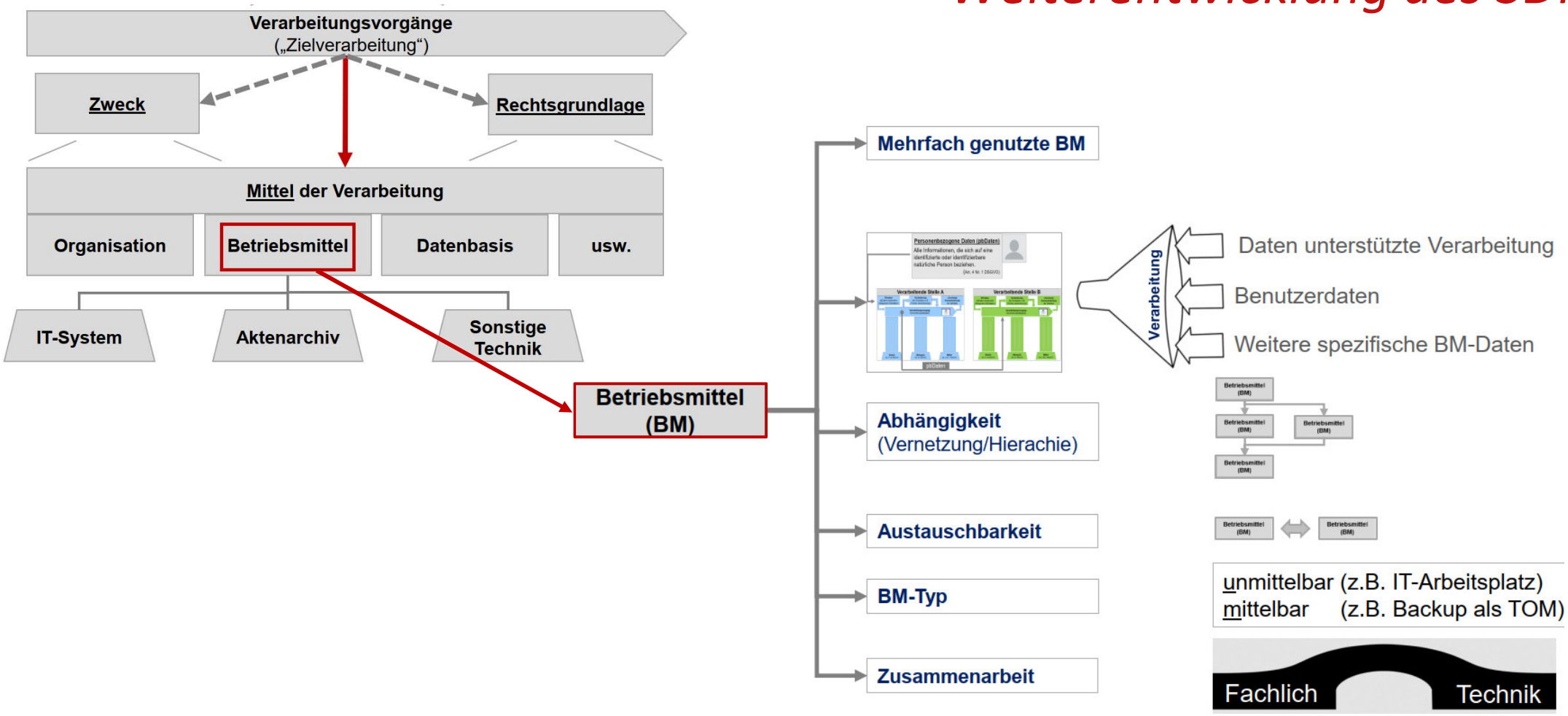
Einführung, Hintergründe und Kontexte zum Erreichen der Gewährleistungsziele

Fachbuch
Buch. Hardcover
2022
xi, 224 S. 14 s/w-Abbildungen, Bibliographien.
Springer Vieweg. ISBN 978-3-658-38879-9

Inhalt

- Einleitung: Wozu Datenschutz?
- Verarbeitung
- Recht
- Gewährleistungsziele
- Datenschutzrisiken
- TO-Maßnahmen
- SDM anwenden
  - Datenschutz prüfen
  - Datenschutz-Folgenabschätzung
  - DS-Management
- Kontext
  - IT-Grundschutz
  - ITIL
- Anhang

3 Verschiedenes
Weiterentwicklung des SDM



Konzept und Grafikentwürfe:
Dr. Chr. Wambsganz (BayLfD)

4 Mit dem SDM(-Würfel) eine Datenschutz-Folgenabschätzung durchführen…

Vielen Dank für Ihre Aufmerksamkeit!

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein
Martin Rost
Telefon: 0431 988-1391
uld32@datenschutzzentrum.de
http://www.datenschutzzentrum.de/