Standarddatenschutzmodell
Grundlagen, Bezüge zu Smart Data

Smart Data

3. Fachgruppentreffen der Fachgruppe Sicherheit

Harald Zwingelberg

Berlin 7. September 2016

Smart Data

Folien: M. Rost, M. Hansen, H. Zwingelberg

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Agenda

1. Was meint „Datenschutz“?

2. Die Entwicklung des Schutzzielekonzepts

3. Operationalisierung der Schutzziele mit Hilfe des

SDM
Standard-Datenschutzmodell

4. Anwendung am Beispiel Transparenz

Datenschutz ein paar Klarstellungen

- Datenschutz ist nicht mit Datenschutzrecht gleichzusetzen.
  Das Datenschutzrecht reagiert auf den Konflikt zwischen Personen und übermächtigen Organisationen.

- Datenschutz ist nicht mit der IT-Sicherheit, etwa dem IT-Grundschutz des BSI, gleichzusetzen.
  Der Datenschutz gilt Betroffenen, nicht Organisationen. Es ist deshalb mit strukturellen Konflikten zwischen Datenschutz und IT-Sicherheit zu rechnen.

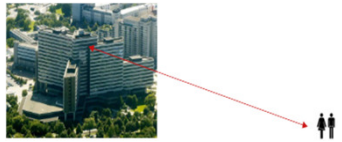
- Das Konzept „informationelle Selbstbestimmung" Voraussetzung für eine moderne Informationsgesellschaft und kein bloßes Zugeständnis an das Bedürfnis nach Privatheit Einzelner

Objektbereich des Datenschutzes

Datenschutz beobachtet, beurteilt und gestaltet die asymmetrischen Machtbeziehungen zwischen Organisationen (Unternehmen / Behörden) und Personen.

Verhältnis IT-Sicherheit - Datenschutz

- **IT-Sicherheit unterstellt methodisch: Jede Person kann ein Angreifer sein!**
  Deshalb müssen Personen in Organisationen Maßnahmen zum Schutz der Informationen und Systeme dulden.
- **Annahme im Datenschutz: Die Organisation selbst ist Angreifer!**
  - Die Organisationen müssen deshalb den Personen nachweisen, dass sie vertrauenswürdig sind.
  - Dies kann u.a. dadurch geleistet werden, dass Organisationen sich nachweisbar an Gesetze und Regeln halten, die Verfahren und Prozesse gesichert beherrschen und diese dokumentiert sind.



EU Grundrechte Charta

„Artikel 1 - Würde des Menschen

Die Würde des Mensch[en] ist [zu achten] und zu sch[ützen].

„Artikel 8 [Schutz personenbezogener Daten]

(1) Jede Pe[rson hat das Recht auf Schutz] die betreffenden personenbe[zogenen Daten].

(2) Diese Da[ten dürfen nur] festgelegte [Zwecke] [mit Einwilligung] Person oder [aufgrund] legitimen Gru[nd] [gesetzlich] Recht, **Ausk[unft]** [über] zu erhalten und die **Berichtigung** der Daten zu erwirken.

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

- Datenschutz ist als Grundrecht europaweit anerkannt
- Hervorgehobene Prinzipien:
  - Rechtmäßigkeit
  - Zweckbindung
  - Betroffenenrechte (Auskunft und Berichtigung)
  - Unabhängige Kontrolle

BVerfG 1983: Volkszählungsurteil

- **BVerfGE 65, 1: Anlass Verfassungsbeschwerde gegen Volkszählungsgesetz**
- **Melderegisterabgleich, Vermischung administrativer und statistischer Funktionen**
- **Wesentliche Inhalte:**

  – *Die automatisierte Datenverarbeitung birgt die Möglichkeit der Auswertung und Verknüpfung von Datenbeständen, die an verschiedenen Orten vorhanden sind:* ***keine belanglosen Informationen***

  – *Möglich wird damit eine vollständige Offenlegung der Privatsphäre der Bürger (Stichwort: „gläserner Bürger")*

  – *[Es] wird der Schutz des Einzelnen gegen unbegrenzte Erhebung […] seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen:*

  => ***Recht auf informationelle Selbstbestimmung***

Grundsatz der Rechtmäßigkeit

Die Verarbeitung personenbezogener Daten ist verboten, sofern nicht erlaubt durch Gesetz oder Einwilligung

- § 4 Bundesdatenschutzgesetz

  „(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat."

- Jede Datenverarbeitung bedarf einer Rechtsgrundlage
  - Gesetz ⇨ § 28 Abs. 1 Satz 1 Nr. 1
  - Andere Rechtsvorschrift ⇨ SGB, TKG, TMG, BerufsO
  - Einwilligung

Volkszählungsurteil

- **BVerfGE 65, 1: Anlass Verfassungsbeschwerde gegen Volkszählungsgesetz**
- **Melderegisterabgleich, Vermischung administrativer und statistischer Funktionen**
- **Wesentliche Inhalte:**

  – *Die automatisierte Datenverarbeitung birgt die Möglichkeit der Auswertung und Verknüpfung von Datenbeständen, die an verschiedenen Orten vorhanden sind:* ***keine belanglosen Informationen***

  – *Möglich wird damit eine vollständige Offenlegung der Privatsphäre der Bürger (Stichwort: „gläserner Bürger")*

  – *[Es] wird der Schutz des Einzelnen gegen unbegrenzte Erhebung […] seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen:*

  => ***Recht auf informationelle Selbstbestimmung***

Was ist wichtig?

Grundrechtseingriffe - und nicht persönliche Risiken oder Schäden - bilden den rechtlichen Rahmen des Datenschutzes.

Auch eine ordnungsgemäß erfolgende Datenverarbeitung ist ein Eingriff in die Grundrechte von Personen. Zwar ist dieser rechtmäßig, bleibt aber ein Eingriff.

Das Konzept der Schutzziele

Schutzziele I (1990er Jahre)

1992: März: Das BSI veröffentlicht die erste Version des „IT-Sicherheitshandbuchs (BSI 7105)"

1994: IT-Sicherheitshandbuch V2 formuliert drei Schutzziele als selbstverpflichtende normative Vorgabe, nämlich Sicherung der **Verfügbarkeit**, **Integrität** und **Vertraulichkeit**.

1995: EU verabschiedet die Datenschutzrichtlinie, in der drei Schutzziele als gesetzliche Vorgaben gefordert sind, nämlich Sicherung der **Transparenz**, **Zweckbindung** und **Datensparsamkeit**.

Schutzziele II
(um das Jahr 2000)

- Garstka / Pfitzmann / Rossnagel empfehlen im „Gutachten zur Modernisierung des deutschen Datenschutzrechts" die Orientierung an „Schutzzielen".
- Die sechs neuen Bundesländer sowie Hamburg, Berlin und NRW weisen in reformierten Landesdatenschutzgesetzen erstmals Schutzziele aus.
- Pfitzmann / Fedderath (Lehrstuhl Informationssicherheit und Datenschutz der TU-Dresden) veröffentlichen einen Artikel zur Systematik von Schutzzielen
- Bezug: „Orange Book" (DoD 1985), Deutsche IT-Sicherheitsbewertungskriterien (1989), ITSEC (1991), Kanadische Kriterien (1992), Common Criteria, ISO/IEC 15408

Schutzziele III (2008)

- Februar 2008: Das Bundesverfassungsgericht fällt das Integritäts- und Vertraulichkeitsurteil

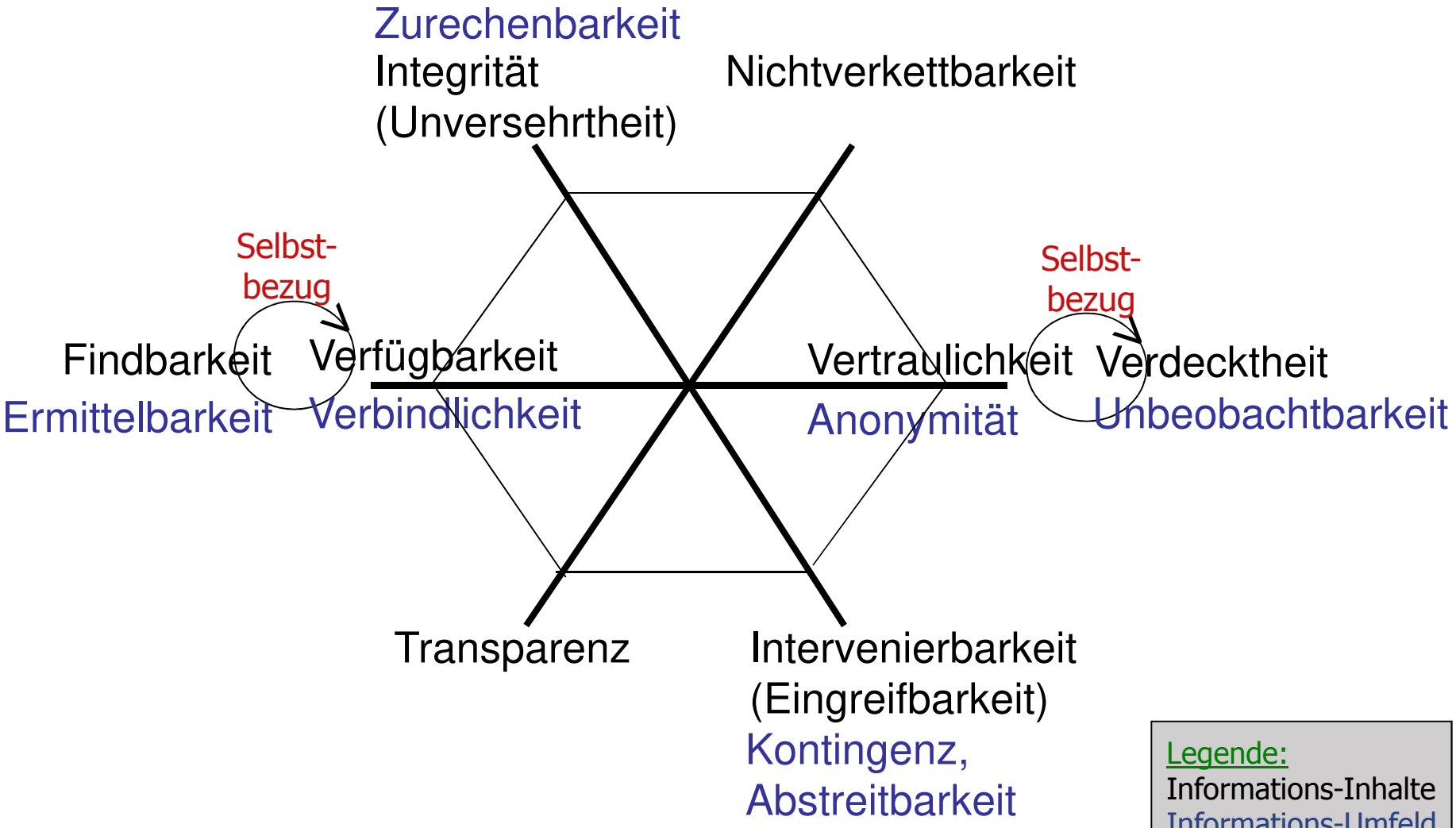
  Der Staat hat die Umsetzung der Schutzziele Vertraulichkeit und Integrität in seinem unmittelbaren Einflussgebiet zu gewährleisten.
  (nach gründlicher Diskussion zwischen Prof. Pfitzmann und Prof. Papier (damaliger Präsident des 2. Senats des BVerfG)).

- November 2008: Prof. Pfitzmann schickt Frau Hansen (ULD) ein internes Arbeitspapier mit einer Kritik an bisherigen Schutzzielkonzepten sowie einen Vorschlag zu einer neuen Systematisierung. Das ULD erkennt den Nutzen für die Beratungs- und Prüfpraxis von Datenschutzbeauftragten.

Schutzziele IV
2009: Kritik am bisherigen Konzept
(gem. Prof. Pfitzmann)

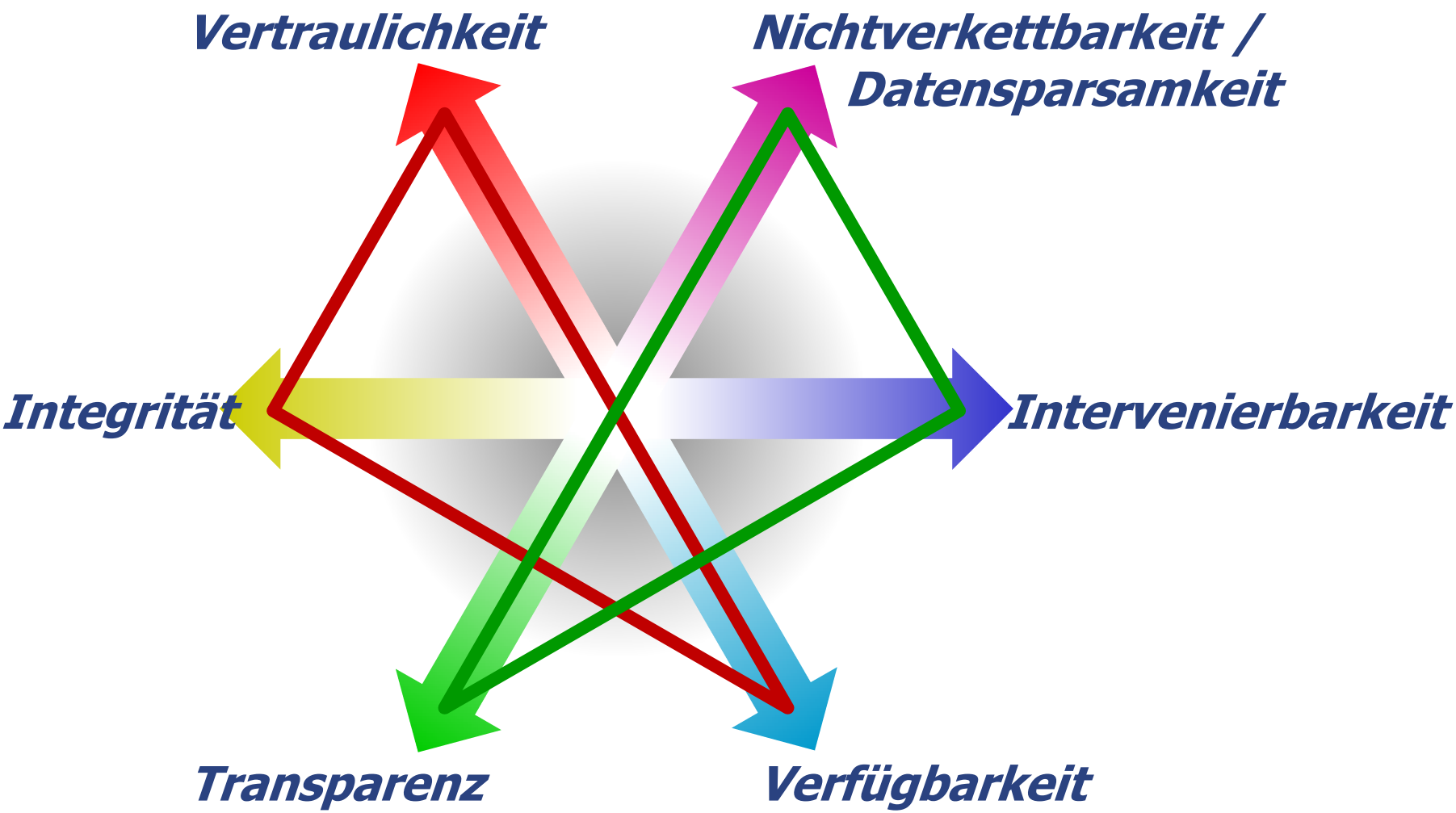
- Fehlende Struktur der Schutzziele
- Wechselwirkungen unbeachtet, d.h. ob und inwiefern sich Schutzziele gegenseitig verstärken oder schwächen, implizieren oder gar gegenseitig ausschließen;
- Bisher keine Überlegungen zur Vollständigkeit der Schutzziele und zu einem diese Ziele erzeugenden System.

Schutzziele V
2009: Schutzziele, vollständiges Set



Legende:
Informations-Inhalte
Informations-Umfeld

Standarddatenschutzmodell (SDM) heute



Schutzziele in modernisierten LDSG

§ 10 Technische und organisatorische Maßnahmen (DSG-NRW)

(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen.

(2) Dabei sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (**Vertraulichkeit**),
2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (**Integrität**),
3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (**Verfügbarkeit**),
4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (**Authentizität**),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (**Revisionsfähigkeit**),
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (**Transparenz**).

Schutzziele in § 5 LDSG S-H

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

- Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können (**Verfügbarkeit**),
- Daten unversehrt, vollständig, zurechenbar und aktuell bleiben (**Integrität**),
- nur befugt auf Verfahren und Daten zugegriffen werden kann (**Vertraulichkeit**),
- die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann (**Transparenz**),
- personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können (**Nicht-Verkettbarkeit**) und
- Verfahren so gestaltet werden, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte nach den §§ 26 bis 30 wirksam ermöglichen (**Intervenierbarkeit**).

Ist das SDM europatauglich?

- Basis bereits des BDSG ist die Datenschutzrichtlinie 1995
- Die Gewährleistungsziele sind eine Abstraktion geltender Rechtsnormen und finden sich vollständig in der DS-GVO und der Polizeirichtlinie wieder.
- Art. 5 DS-GVO arbeitet ebenfalls mit einem Konzept von Gewährleistungszielen
- Art. 25 DS-GVO setzt auf Datenschutz durch Tehnikeinsatz. Dafür ist eine Metrik zu Bewertung erforderlich.

Schutzziele in der DSGVO

Art 5, Abs 1., DS-GVO „Personenbezogene Daten müssen"

(a) „... in einer für die Person nachvollziehbaren Weise verarbeitet werden ... (**Transparenz**)."
(b) „... für festgelegte eindeutige und rechtmäßige Zwecke erhoben werden ... (**Zweckbindung**)."
(c) „... auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**Datenminimierung**)."
(d) „... damit personenbezogene Daten ... unverzüglich **gelöscht** oder **berichtigt** werden"
(e) „... **Integrität** und **Vertraulichkeit**".

Schutzziele:

Transparenz

Nicht-Verkettbarkeit

Datensparsamkeit

Intervenierbarkeit

Integrität
Vertraulichkeit

Verfügbarkeit fehlt

Gewährleistungsziele in der DS-GVO

Ziel	Vertrau-lichkeit	Verfügbar-keit	Integrität	Nicht-Verkettbar keit	Transpa-renz	Inter-venier-barkeit
Norm der DS-GVO	5 (1) f, 28 (3) b, 32	13, 15, 20, 32	5 (1) d, 5 (1) f, 32	5 (1) b, 5 (1) c, 5 (1) e, 25, 32	5 (1) a, 12, 13, 14, 15, 32, 33, 34	12/2, 15 (1) e, 16, 17, 18, 19, 20, 21, 22 (3)

Gewährleistungsziele in der JI-Richtlinie

Ziel	Vertrau-lichkeit	Verfügbar-keit	Integrität	Nicht-Verkettbarkeit, Datensparsamk.	Transpa-renz	Inter-venier-barkeit
Norm der JI-Richtl.	4 (1) (f) 5 8 9 20 22 (3) (b) 29	4 (1) (f) 12 13 14 20 p. 1 29	4 (1) (d), (f) 6 7 20 (1) 24 25 29	4 (1) (b) - (f), (2) (a), (b), (3) 5 8 9 20 29	4 (4) 13 14 17 (3) 19 (1) 20 24 25 28 30 31	4 (1) (d) 11 (1), (2) 12 (2) 13 14 (e) 16 17 18 20 22 (3) (d)

Projektergebnis aus:

VALCRI
VISUAL ANALYTICS FOR SENSE-MAKING IN CRIMINAL INTELLIGENCE ANALYSIS

Was ist wichtig?

- Schutzziele / Gewährleistungsziele systematisieren die Anforderungen des grundrechtlich gewährten Datenschutzes.
- Abstraktion bestehender Anforderungen aus Gesetzen
- „Brückenschlag" zwischen Technik und Recht
- Zukunftsfähig da kompatibel DS-GVO und Richtlinie

Praktischer Einsatz der Schutzziele mit Hilfe des Standard-Datenschutzmodells

Prüfgegenstand: Verfahren

- Was wird geprüft: Verfahren
- **Verfahrens-Komponenten**
  Ein Verfahren besteht aus drei zu betrachtenden Komponenten:
- Daten (und Datenformaten)
- IT-Systemen (und Schnittstellen)
- Prozessen (und adressierbaren Rollen)

Schutzbedarf
Sicht aus der Betroffenenperspektive!

(bislang interner Entwurf, angenommen vom AK-Technik (Sitzung in 2016/03))

„Datenschutzrechtlich maßgeblich sind nicht die zu verhindernden Schäden, die aus Mängeln der Informationssicherheit herrühren können, sondern ist die Eingriffsintensität, die durch die Verarbeitung von Personendaten auf Seiten der Organisation gegenüber einer Person gegeben ist."

Schutzbedarf
Sicht aus der Betroffenenperspektive!

(bislang interner Entwurf, angenommen vom AK-Technik (Sitzung in 2016/03))

- **Normaler Schutzbedarf**
  gilt mindestens für jedes personenbezogene Verfahren.

- **Hoher Schutzbedarf**
  für ein personenbezogenes Verfahren besteht dann, wenn Betroffene von den Entscheidungen bzw. Leistungen einer Organisation abhängig sind und wenn eine Organisation
  - mit einer weitreichenden Eingriffsintensität Daten verarbeitet, was zu erheblichen Konsequenzen für den Betroffenen führen kann,
  - Daten verarbeitet, welche gesetzlich als besonders schutzwürdig ausgewiesen sind,
  - keine funktionierenden Möglichkeiten der Intervention und des Selbstschutzes für Betroffene bereitstellt.

- **Sehr hoher Schutzbedarf**
  ist gegeben bei Gefahr für Leib und Leben.

Schutzmaßnahmen
Beispiele aus dem Referenzkatalog

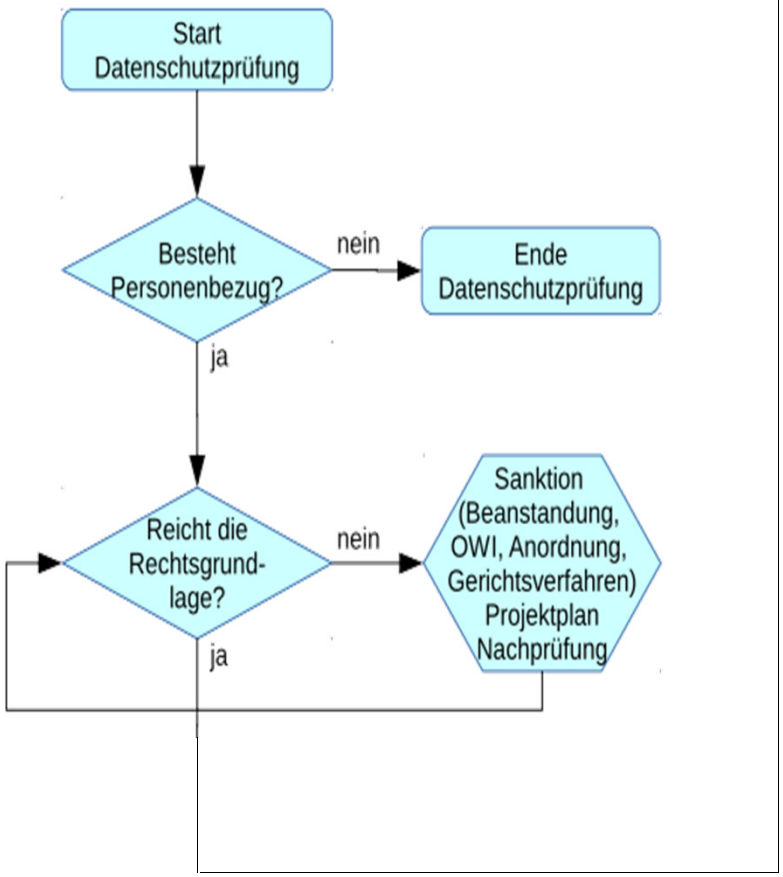
- Datensparsamkeit: Reduzierung erfasstet Attribute betroffener Personen und der Verarbeitungsoptionen / Reduzierung der Möglichkeiten der Kenntnisnahme vorhandener Daten
- Verfügbarkeit: Backup und Restore / Vertretungsregeln
- Vertraulichkeit: Verschlüsselung von Datenbeständen und Kommunikationen / Rechte- & Rollenkonzept
- Integrität: technischer Integritätsschutz (elektronische Signaturen und deren Prüfungen) / Soll-Definitionen für Prozesse, mit Ereignisdefinitionen zur Prüfbarkeit von Soll-Abweichungen
- Transparenz: Herstellung von Prüfbarkeit durch Spezifikation, Dokumentation und Protokollierung
- Nichtverkettbarkeit: Trennung / Isolierung unter der inhaltlichen Maßgabe der Umsetzung informationeller Gewaltenteilung / Pseudonymisierung / Anonymisierung
- Intervenierbarkeit: Auskunft, Berichtigung, Sperrung, Löschung, Widerspruch („Außenschnittstelle" einer Organisation) / Prozesse einer Organisation zur Erkennung und Bearbeitungen von Störungen, Problembearbeitungen und Änderungen

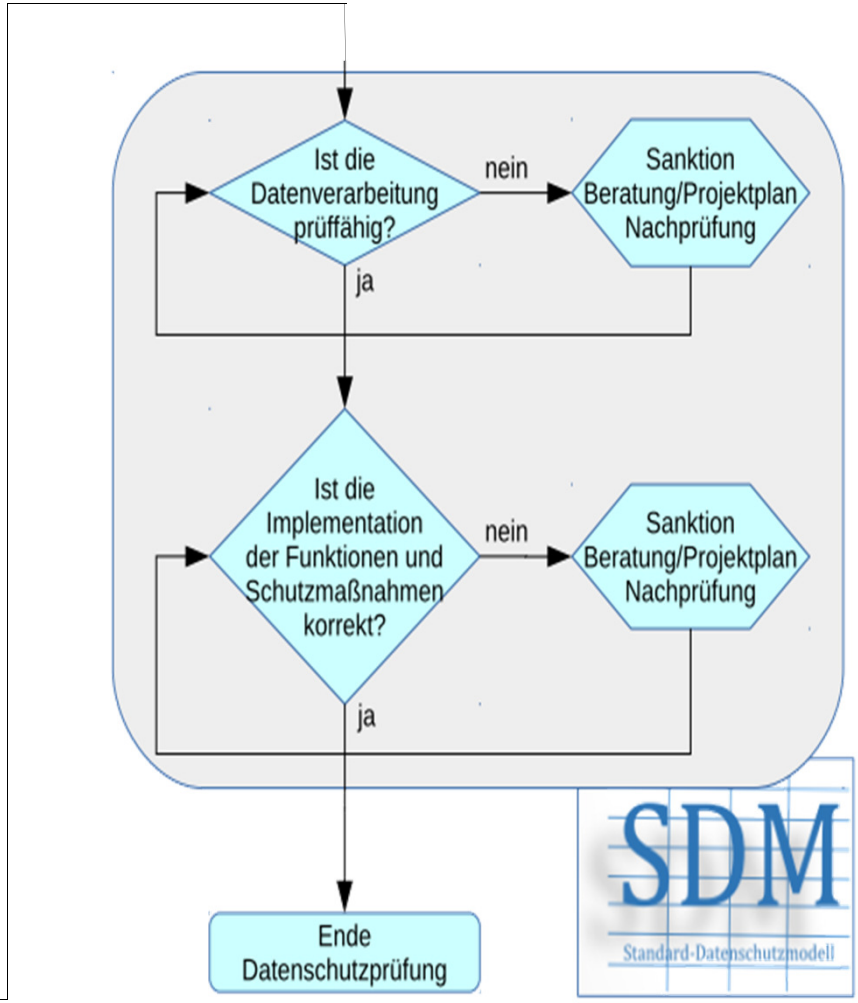
Update des Katalogs ist in Arbeit.

Funktion des SDM

Schutzziele, und deren Umsetzung durch das SDM, koppeln Recht und Technik, lassen sich wissenschaftlich untersuchen sowie deren Umsetzung, vermittelt über die Schutzmaßnahmen, betriebs-wirtschaftlich kalkulieren.

Prüfablauf Datenschutz





Betriebskonzept für das SDM

- Zweck: Kontrollierte Änderung bzw. Fortschreibung
- Eigentümerin: Konferenz der Datenschutzbeauftragten
- Entwicklung und Pflege: Arbeitskreis Technik
- Bearbeitung des SDM-Handbuchs einschl. Referenz-Schutzmaßnahmen;
- Bearbeitung von Änderungsanträgen zum SDM;
- Sicherung der Qualität von Arbeitsergebnissen;
- Folgeauflagen des SDM-Handbuchs;
- Projektmanagement, das umfasst:
  - Bereitstellung eines Single Point of Contact (Service Desk) für Beratungen und CRs zum SDM
  - Betrieb von CR-Verfolgung
  - Moderation von Diskussionen

Mehr zum Thema

- 2015-10: "SDM-Handbuch" Version 0.9a des Handbuchs wurde im Oktober 2015 von der Konferenz der Datenschutzbeauftragten empfohlen
- V1.0 ist in der Abschlussphase
- Englische Übersetzung geplant
- Mehr: www.datenschutzzentrum.de/SDM

Was ist wichtig?

- SDM hat sich im Prüf- und Beratungsgeschäft bewährt
- SDM verbindet Sichtweisen aus rechtlicher, technischer, wirtschaftlicher und wissenschaftlicher Perspektive
- SDM gestattet Blick auf Wechselwirkungen zwischen Maßnahmen und Zielen. Ggf. kann das Nichterreichen eines Ziels durch Maßnahmen zugunsten der anderen Ziele erreicht werden.

Einsatz bei der Entwicklung von Prozessen / Produkten Beispiel: Transparenz

Gewährleistungsziel Transparenz

Transparenz bezeichnet die Anforderung, dass sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme hat.

Quelle: Standarddatenschutzmodell, S. 13.

Gewährleistungsziel Transparenz und Big Data

- Informationen sind vollständig, präzise und allgemeinverständlich den Betroffenen zugänglich zu machen, Art. 12 DS-GVO.
- Katalog der erforderlichen Informationen in der Art. 13
- Bei Erhebung beim Betroffenen ist direkt zu informieren.
- Zwecke, Speicherdauer oder Kriterien für Festlegung der Dauer

⇒ Löschfristen und Zwecke sind vorab zu definieren. Das gilt zwar schon jetzt ist aber künftig proaktiv zu beauskunften.

Gewährleistungsziel Transparenz und Big Data

- Bei Erhebung „hinter dem Rücken“ ist nachträglich zu informieren, Art. 14 DS-GVO

- Information bei Erhebung ohne Kenntnis der Betroffenen
  - Aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen, Art. 14 (2) (f) DS-GVO.

  ⇒ Auch Daten aus öffentlichen Quellen lösen damit wohl die Informationspflicht aus.

  ⇒ Erforderlich daher: Prozess, zur Information der Betroffenen

  ⇒ Angaben über Rechtsgrundlage, Einwilligung, Quelle der Erhebung sollten mit den Daten zusammen zu vorgehalten werden

  ⇒ Offen: Welche Methoden der Information dürfen genutzt werden?

  ⇒ Offen: Vermittelnde Rechtsauffassung für selektierte use cases?

Ausnahmen zugunsten von Big Data?

- Transparenz ist kompliziert? Ja.
- Auswege über die Ausnahmen in Art. 14 (5) (b) denkbar?
  - Auskunftspflicht entfällt, sofern „sich die Erteilung […] als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde […]"
    Regelbeispiele dieser Ausnahme: insbesondere für öffentliche Archive, Forschungszwecke und Statistik. Wohl kein Privileg für Datenverarbeitung zur rein gewinnorientierten (Werbe-)Zwecken.
  - Jedenfalls wird regelmäßig kein unverhältnismäßiger Aufwand vorliegen. Alle Prozesse für die Umsetzung von Betroffenenrechten müssen ohnehin etabliert sein. Gerade bei Big Data kann (Rechen-)Aufwand eher nicht berücksichtigt werden.
- Weitere Optionen und ggf. vermittelnde Rechtsmeinungen in künftigen Kommentierungen / Aufsätzen zur DS-GVO.

Gewährleistungsziel Transparenz und Big Data

- Datenschutz durch Technikgestaltung als Umsetzungsvorschläge

⇒ Informationen über Rechtsgrundlage der Einwilligung und Quelle der Erhebung sind mit den Daten mitzuführen.

⇒ Auch um die Rechte auf Auskunft, Berichtigung und Löschung umzusetzen (Intervenierbarkeit) bedarf es entsprechender Prozesse, um Daten eines Betroffenen zu lokalisieren.

⇒ Es ist ein standardisierter Prozess sinnvoll, um die Daten mit den erforderlichen Meta-Informationen anzureichern. Dazu gibt es bereits Ausarbeitungen, Stichwort: „sticky policies".

⇒ Zugriffsschutz, Protokollierung, Rollenkonzepte

Gewährleistungsziel Transparenz

- **Erweiterter Transparenzbegriff u.a. für Ermittlungsbehörden**

VALCRI
VISUAL ANALYTICS FOR SENSE-MAKING IN CRIMINAL INTELLIGENCE ANALYSIS

  - Nicht nur Datenschutzperspektive sondern z.B. auch (Straf-)Prozessrecht – Vollständige Nachvollziehbarkeit einer späteren Verurteilung von der Erhebung erster Indizien bis zum Urteil

  - Ethik – Entscheidungen durch Big Data müssen nachvollziehbar sein.

Hinweis: im Polizeibereich gilt nicht die DS-GVO sondern die zeitgleich verabschiedete Datenschutz Richtlinie.

Was ist wichtig?

- Die partielle Öffnung der Zweckbindung in der DS-GVO kann Smart Data Anwendungen unterstützen, ist aber keine Universalerlaubnis:
  - Transparenzanforderungen wurden gestärkt und beeinflussen die Rechtmäßigkeit der weiteren Datenverarbeitung. (Transparenz)
  - Einflussmöglichkeiten der Betroffenen gestärkt (Intervenierbarkeit)
  - Privacy by Design: Technische Schutzmaßnahmen nach Stand der Technik erforderlich

Quellen

Dieser Vortrag beruht auf laufenden Arbeiten aus drittmittelgeförderten Forschungsprojekten am ULD:

iTESA – intelligent Traveller Early Situation Awareness
http://www.smart-data-itesa.de

Forum Privatheit
https://www.forum-privatheit.de/form-privatheit-de/index.php

VALCRI – Visual Analytics for sense-making in Criminal Intlligence Analysis
http://valcri.org

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

EUROPEAN COMMISSION

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt:
Harald Zwingelberg
hzwingelberg@datenschutzzentrum.de
www.datenschutzzentrum.de
0431/988-1222