Datenschutz und Sicherheit

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

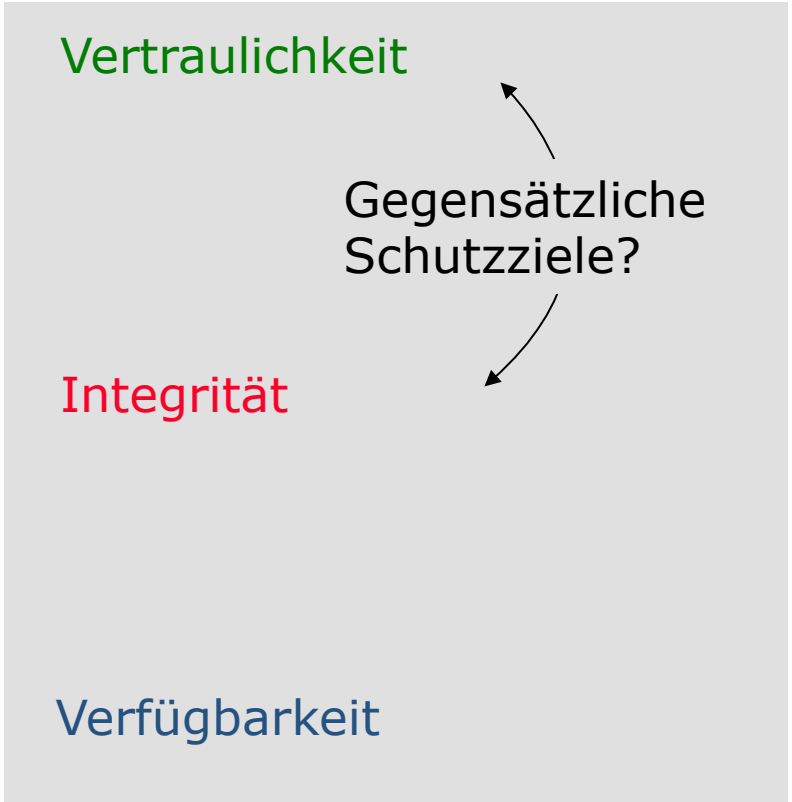
12. Tagung der DFN-Nutzergruppe Hochschulverwaltung
"Sicherheit trotz(t) IT" vom 18. - 20. Mai 2015 an der
Ruhr-Universität Bochum

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Schutzziele

Voydock, Kent 1983

- Klassische IT-Sicherheit berücksichtigt im Wesentlichen Risiken, die durch *regelwidriges Verhalten* in IT-Systemen entstehen.



unbefugter Informationsgewinn

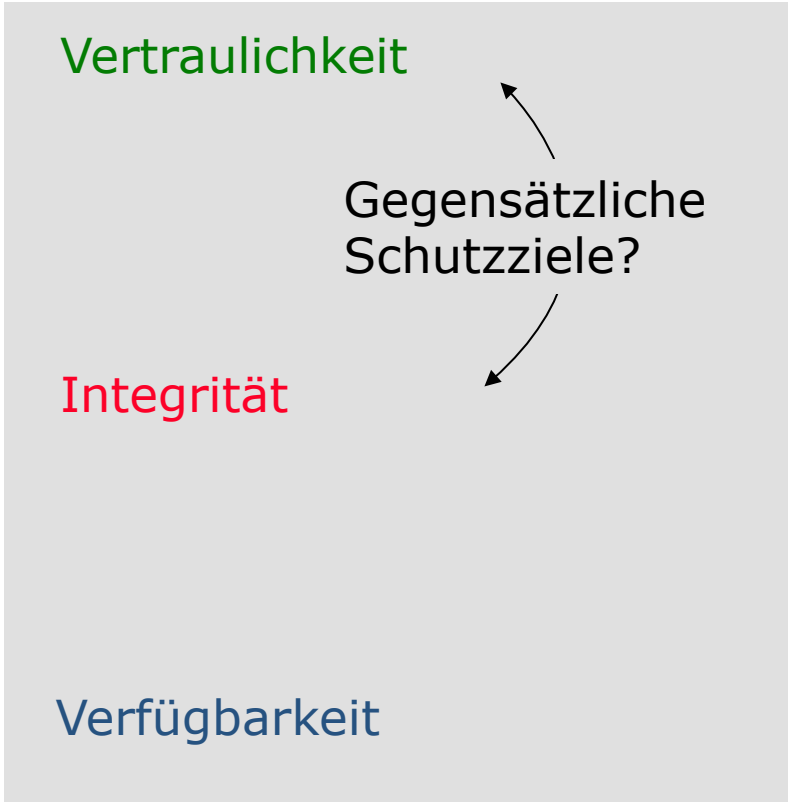
unbefugte Modifikation

unbefugte Beeinträchtigung der Funktionalität

Mehrseitige Sicherheit

Müller et. al. 1997

- Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte.

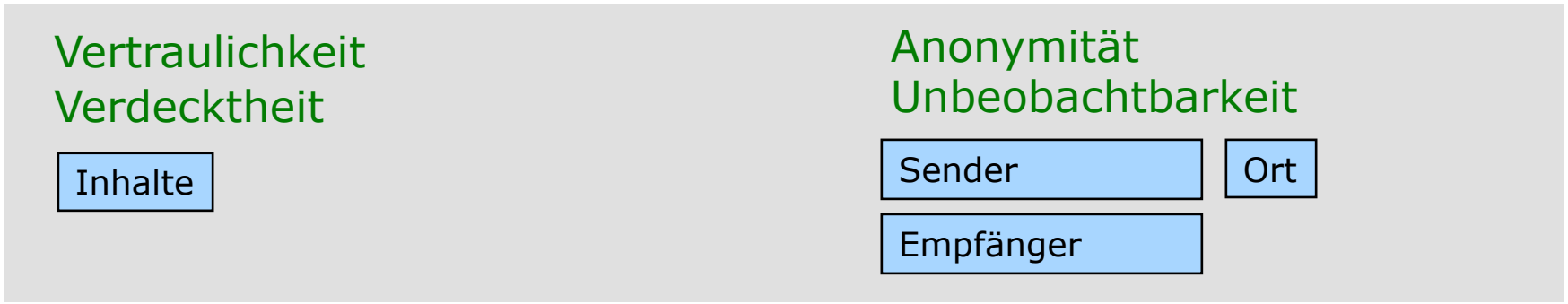


- Voraussetzung
  - regelwidriges Verhalten hält Systeme und Nutzer schadlos
- Ziel
  - gegensätzliche Sicherheitsinteressen werden erkannt, Lösungen ausgehandelt und durchgesetzt

Schutzziele der mehrseitigen Sicherheit

Kommunikationsgegenstand Was?, Worüber? Inhaltsdaten	Kommunikationsumstände Wann?, Wo?, Wer? Verkehrsdaten
Vertraulichkeit Verdecktheit Inhalte	Anonymität Unbeobachtbarkeit Sender, Ort, Empfänger
Integrität Inhalte	Zurechenbarkeit Rechtsverbindlichkeit Absender, Bezahlung, Empfänger
Verfügbarkeit Inhalte	Erreichbarkeit Nutzer, Rechner

Vertraulichkeit: Schutzziele und Angreifermodell



- Outsider
  - Abhören auf Kommunikationsleitungen
  - Verkehrsanalysen

- Insider
  - Netzbetreiber oder bösartige Mitarbeiter (Verkehrsprofile)
  - Staatliche Organisationen (insb. fremde)

Vertraulichkeit: Verfahren und Algorithmen

Was wird geschützt?

Beispiele für Verfahren

Beispiele für Algorithmen

Inhaltsdaten

Vertraulichkeit

Verschlüsselung

Inhalte

DES, 3-DES, OTP, IDEA, AES, RSA, ElGamal, …

Verdecktheit

Steganographie

Inhalte + Existenz

F5, …

Verkehrsdaten

Anonymität Unbeobachtbarkeit

Sender

Ort

Empfänger

Web-Anonymisierer, Remailer, anonyme Zahlungssysteme

Pseudonyme, Proxies, umkodierende Mixe, DC Netz, Private Information Retrieval, …

Integrität und Zurechenbarkeit, Rechtsverbindlichkeit

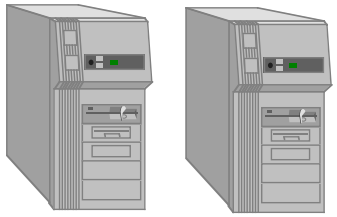
Verfahren

Algorithmen

Inhaltsdaten	Kommunikationsumstände Wann?, Wo?, Wer?
Integrität	Zurechenbarkeit Rechtsverbindlichkeit auch: Authentizität Unabstreitbarkeit
Inhalte	Absender, Bezahlung
Message Authentication Codes	Empfänger
Challenge-Response-Authentikation	Digitale Signaturen
	RSA, ElGamal, …

Verfügbarkeit: Redundanz und Diversität

- Redundanz
  - Mehrfache Auslegung von Systemkomponenten
  - Bei Ausfall übernimmt Ersatzkomponente



Beispiel: Doppelung

- Diversität
  - Verschiedenartigkeit der Herkünfte
  - Tolerieren von systematischen Fehlern und verdeckten trojanischen Pferden
  - Unabhängige Entwicklung von redundanten (Software)-Komponenten

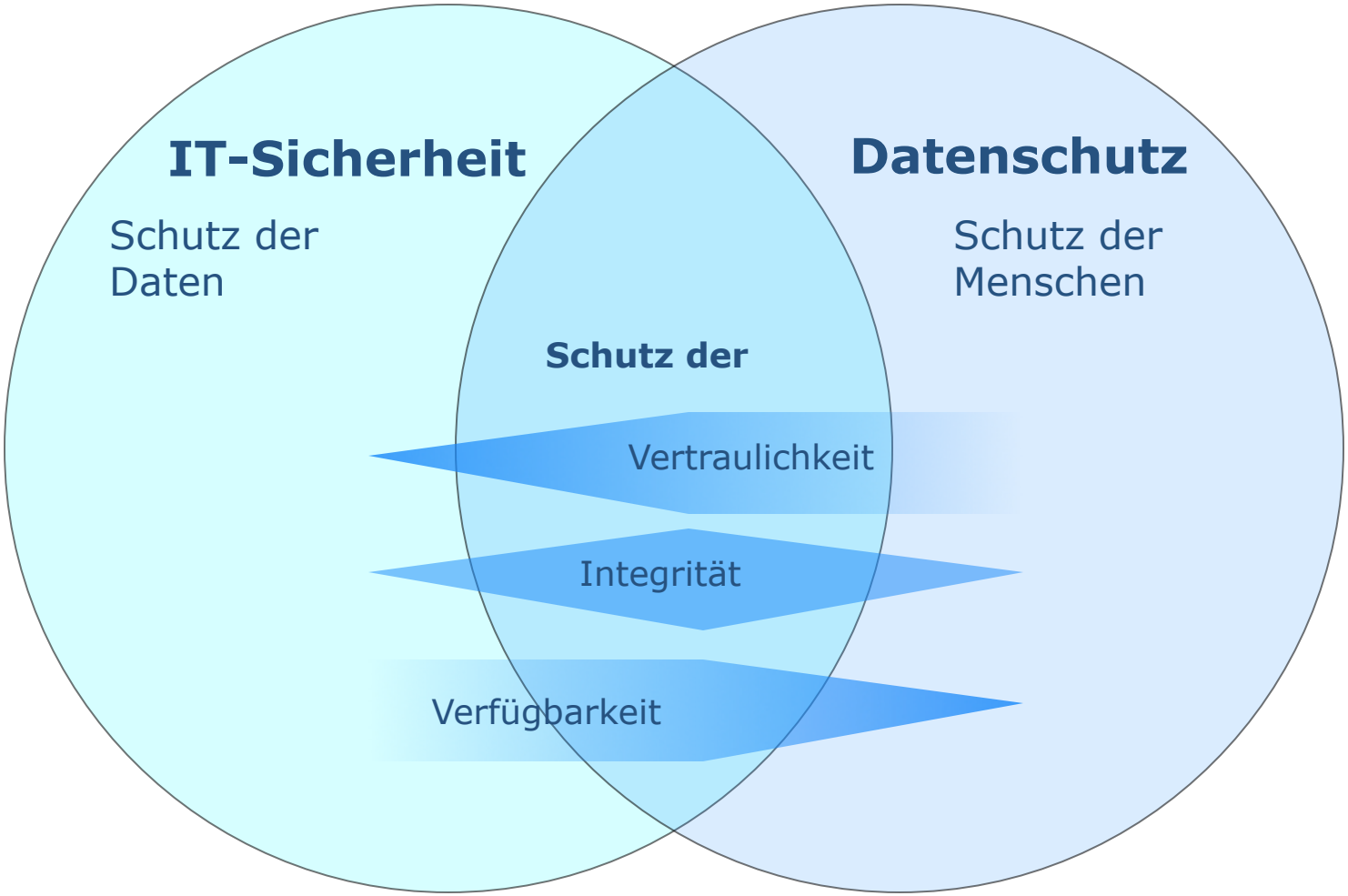
Verfügbarkeit

Inhalte

Erreichbarkeit

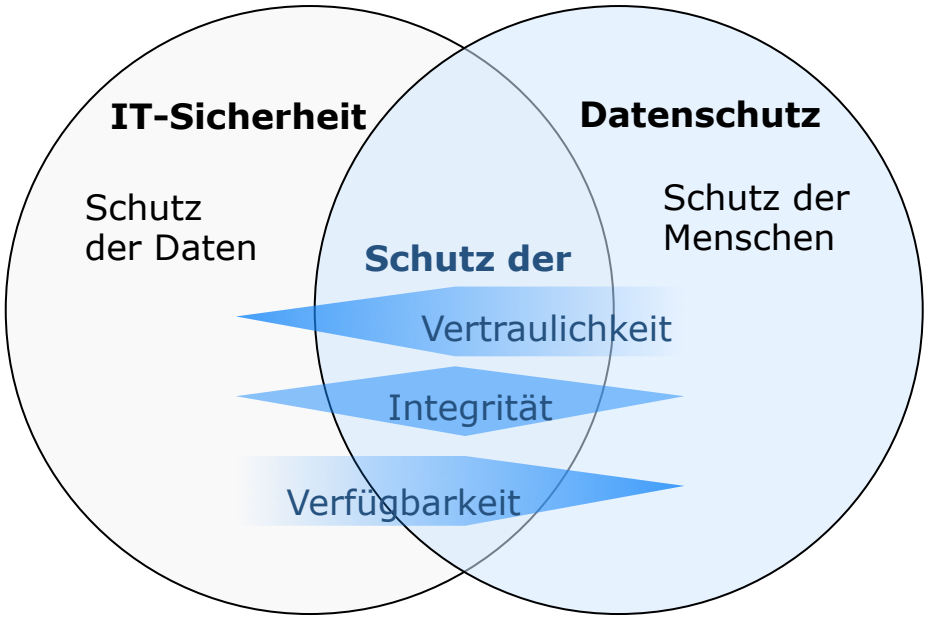
Nutzer | Rechner

Verknüpfung von Sicherheit und Datenschutz



BDSG § 9 Technische und organisatorische Maßnahmen

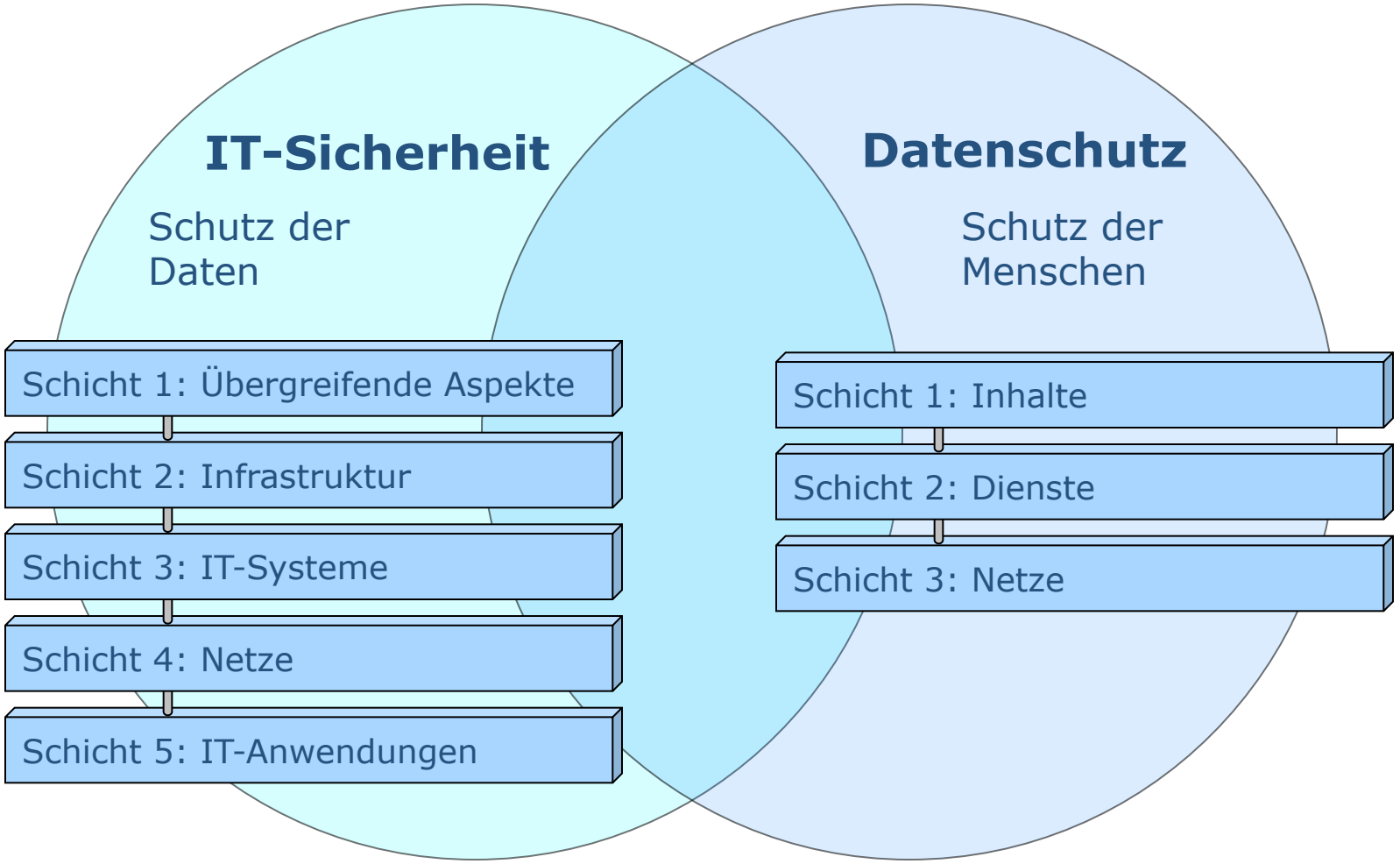
- Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.



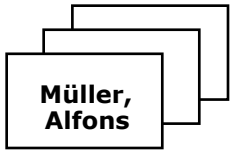
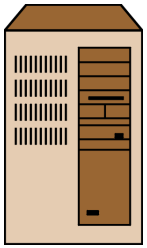
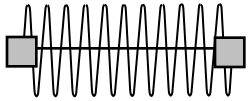
Anlage zu § 9 Abs. 1 BDSG

1. Zutrittskontrolle (räumlicher Zutritt, Gebäude)
2. Zugangskontrolle (Benutzung, Passwort)
3. Zugriffkontrolle (Berechtigung, Administratoren)
4. Weitergabekontrolle (Transport, Netze)
5. Eingabekontrolle (Nutzer-Protokoll)
6. Auftragskontrolle (Outsourcing, Wartung)
7. Verfügbarkeitskontrolle (Zerstörung)
8. Trennungsgebot (Zwecktrennung)

Verknüpfung von Sicherheit und Datenschutz



«Drei Schichten» des Datenschutzes in Kommunikationsnetzen

Ebene der Anwendung/Inhalte		z.B. Kundendaten nach Warenbestellung im virtuellen Kaufhaus	**BDSG, LDSG**
Ebene der Dienste «Internet»		z.B. **Clickstream** nach Zugriff auf den Web-Server	**TMG**
Ebene der Netze «Telekommunikation»		z.B. **ISDN-Verkehr** über die Leitungen der Telekom zwischen dem Nutzer und dem Access-Provider	**TKG**

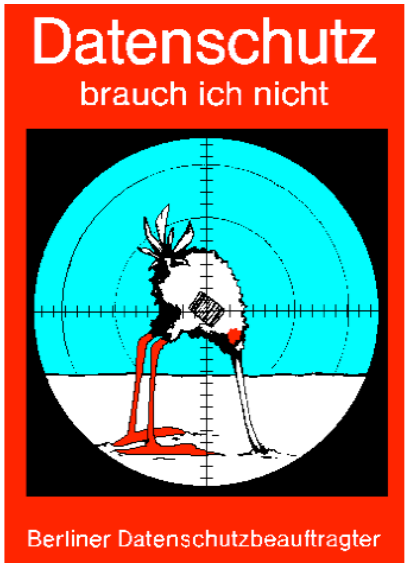
Grundsätze des Datenschutzes und Rechte der Betroffenen

- Grundsätze des Datenschutzes
  - Verbot mit Erlaubnisvorbehalt
  - Einwilligung des Betroffenen
  - Grundsatz der Zweckbindung
  - Erforderlichkeitsgrundsatz (Verhältnismäßigkeit)

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist zulässig, soweit diese durch ein Gesetz oder eine andere Rechtsvorschrift erlaubt ist oder der Betroffene eingewilligt hat.

- Rechte der Betroffenen
  - Recht auf Auskunft
  - Recht auf Berichtigung, Sperrung oder Löschung
  - Widerspruchsrecht des Betroffenen gegen die Datenverarbeitung
  - Recht auf Anrufung des BfD und anderer Kontrollinstitutionen
  - Recht auf Schadenersatz

www.datenschutz.de
Virtuelles Datenschutzbüro



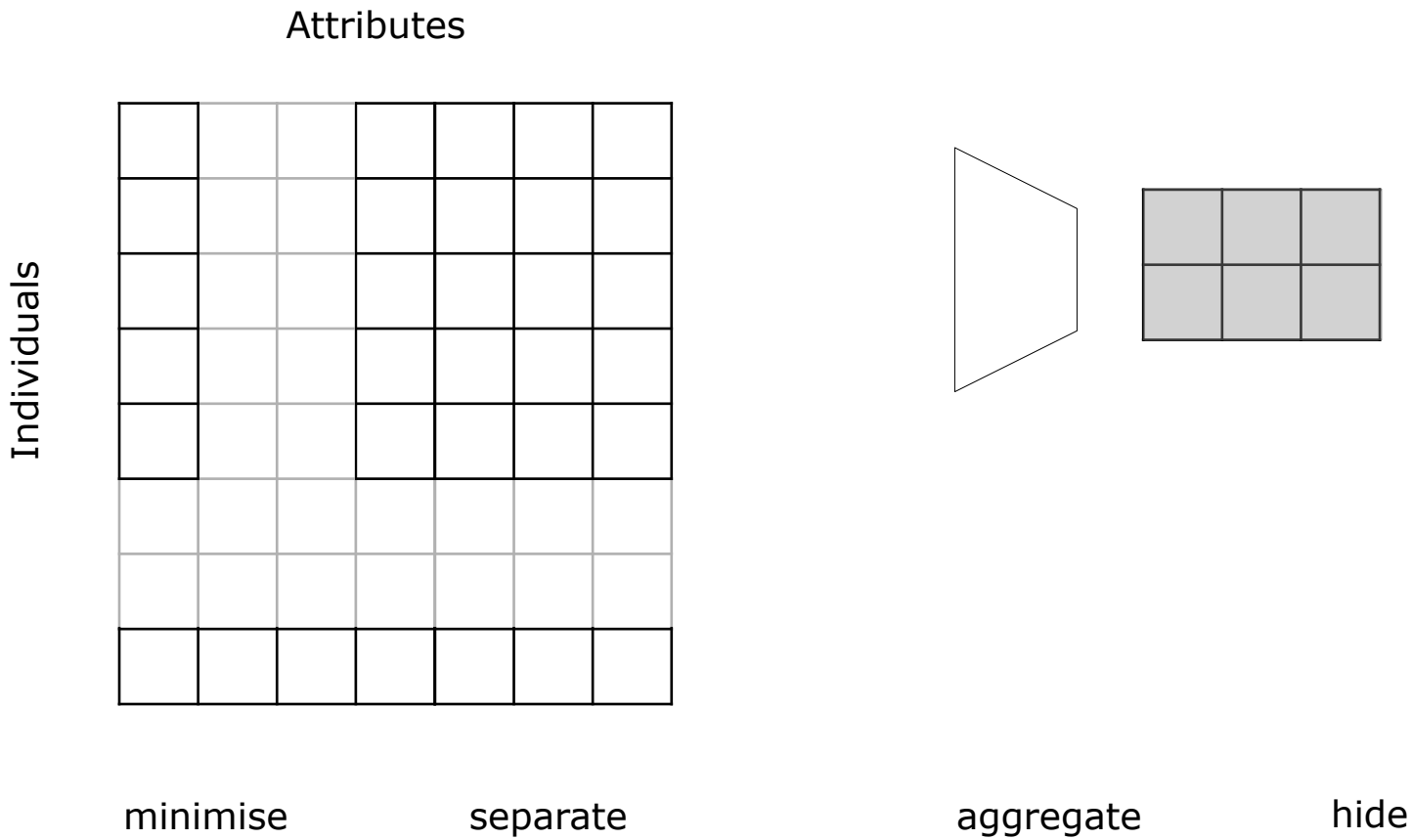
Goldene Regeln zur Umsetzung von Datenschutz

- Aus Sicht der IT-Sicherheit:
  - Informieren (Transparenz)
  - Auskunftsverfahren etablieren
  - Einwilligung, wo nötig
  - Weniger (speichern) ist mehr (Datenschutz)
  - Regelmäßige Sensibilisierung (wie Umwelt- und Arbeitsschutz)
  - Sanktionen bei Verstößen klarmachen
  - Aber: Kontrollieren und beraten, nicht gleich bestrafen!

- Immer fragen: Was ist die Grundlage der Erhebung/Verarbeitung/Speicherung?
  - Einwilligung?
  - Gesetzliche Vorgabe?
  - Aufrechterhaltung des laufenden Betriebs? (IT-Sicherheit)

Privacy design strategies

nach: Hoepmann, 2013



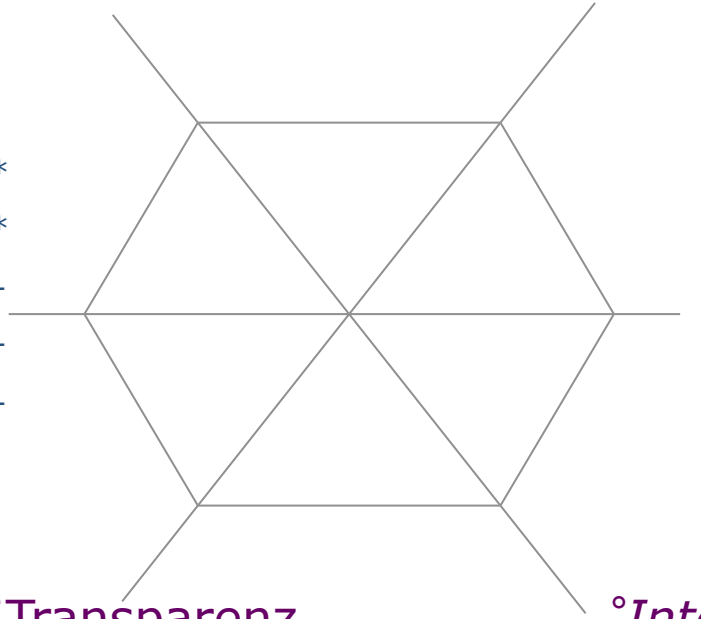
Privacy design strategies

nach: Hoepmann, 2013

- Technisch
  - Minimise: Nur notwendige Daten speichern und verarbeiten
  - Separate: Daten verteilt verarbeiten und speichern
  - Aggregate: Daten auf das notwendige Maß zusammenfassen
  - Hide: Daten nicht in offener Form speichern

- Organisatorisch
  - Enforce: Durchsetzung einer Datenschutz-Policy (access control)
  - Inform: Betroffene über Datenverwendung informieren (P3P)
  - Control: Eingriffsmöglichkeit der Betroffenen (informed consent)
  - Demonstrate: Überprüfbarkeit (privacy management, logging)

Schutzziele in Anlehnung an Bock und Rost, 2011



*Integrität (Unversehrtheit)**
Zurechenbarkeit+
Rechtsverbindlichkeit+

°*Nichtverkettbarkeit (Zweckbindung, Zwecktrennung)*

*Verfügbarkeit**
Findbarkeit*
Erreichbarkeit+
Ermittelbarkeit+
Verbindlichkeit+

**Vertraulichkeit*
*Verdecktheit
+Anonymität
+Unbeobachtbarkeit

°Transparenz

°*Intervenierbarkeit (Eingreifbarkeit)*
+Kontingenz
+Abstreitbarkeit

kursiv = *elementare Schutzziele*
normal = abgeleitete Schutzziele
* = Schutz der Inhaltsdaten
+ = Schutz der Verkehrsdaten
° = spezifische Datenschutz-Schutzziele

x ——— y
Dualität

Recht auf informationelle Selbstbestimmung

«Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den *Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten* voraus. …

Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. *Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.»*

aus dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 1. BvR 209/83 Abschnitt C II.1, S. 43

Abgrenzung von IT-Sicherheit und Datenschutz

- IT-Sicherheitsmanagement
  - IT-Sicherheitsmanagement versucht, die mit Hilfe von Informationstechnik (IT) realisierten Produktions- und Geschäftsprozesse in Unternehmen und Organisationen systematisch gegen beabsichtigte Angriffe (Security) und unbeabsichtigte Ereignisse (Safety) zu schützen.

- Datenschutz
  - Mit dem Begriff Datenschutz wird das Recht des Einzelnen auf informationelle Selbstbestimmung umschrieben. «Das Grundrecht gewährleistet [...] die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.» (BVerfG) Eine Organisation hat technisch-organisatorische Maßnahmen zu treffen, um dieses Recht zu gewährleisten.