Vorlesung Datenschutz CAU SS 2026

Datenschutz und Technik I/II

Schutz- und Gewährleistungsziele Datenschutz- und Sicherheitsmanagement, BSI-Grundschutz

Dr. Thomas Probst
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel
thomas.probst@datenschutzzentrum.de

Hinweis: Diese Folien wurden von dem Dozenten für die Vorlesung erstellt und nicht mit dem ULD abschließend abgestimmt.

Kennen Sie rechtliche Regelungen zum Datenschutz?

Beispiele

- Datenschutzgrundverordnung (DSGVO)
- Richtlinie Datenschutz Polizei + Sicherheit + Justiz (JI-Richtlinie)

- Bundesdatenschutzgesetz (BDSG)
- Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)

- Landesdatenschutzgesetze (LDSG XX)

Abgrenzung zu anderen rechtlichen Regelungen im Bereich „Daten"

- Welche kennen Sie?

Beispiele

- Informationssicherheit
  - BSI-Gesetz, Cyberresiliance-Act, NIS2, KRITIS
  - Regelungen der BaFin im Bereich Banken und Versicherungen (BAIT, VAIT);

    zunehmend ersetzt durch europäische Regelungen (DORA, Digital Operational Resilience Act)
- Urheberrecht
- KI (AI-Act)
- Wettbewerbsrecht, Digital Market Act

Kennen Sie andere Regelwerke außer Rechtsnormen?

Begriffsklärung: Informationssicherheit

Begriffe

- Informationssicherheit = ?
- Datensicherheit = ?
- Datenschutz = ?

Begriffe

Informationssicherheit ≈ Datensicherheit;

Teilgebiete:

- IT-Sicherheit
- Sicherheit von nicht-elektronischen Informationen

Die Informationssicherheit schützt Informationen (und zur deren Verarbeitung eingesetzter Infrastrukturen und Systeme) der Organisation.

Begriffe

Datenschutz

- Datenschutz schützt das Recht **betroffener Personen** auf informationelle Selbstbestimmung (Grundrechtsschutz)

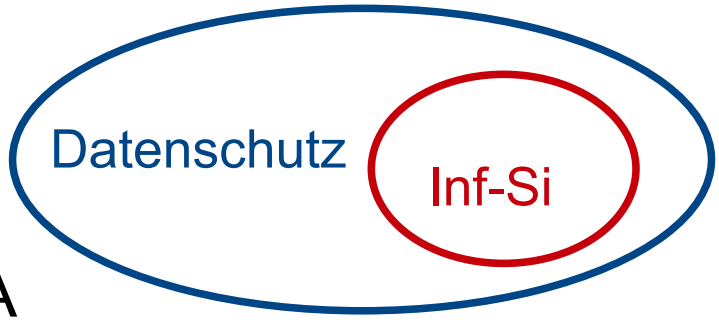
- [in Publikationen wird manchmal „Datenschutz“ anstelle von „Informationssicherheit“ verwendet. Manchmal werden im Englischen mit „data protection″ auch Backupmechanismen bezeichnet.]

Datenschutz und Informationssicherheit

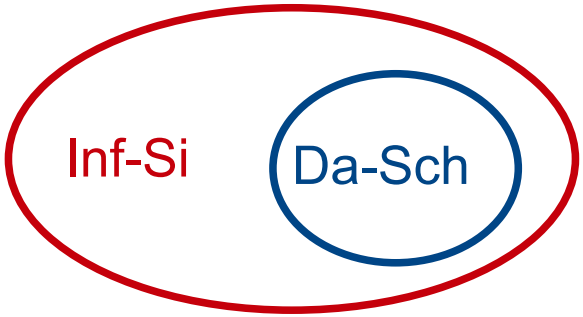
- Datenschutz:
  Schutz der Menschen vor Missbrauch ihrer personenbezogenen Daten

- Informationssicherheit/Datensicherheit:
  Schutz der Informationen/Daten(-verarbeitung) vor unberechtigten Zugriffen und vor Zerstörung

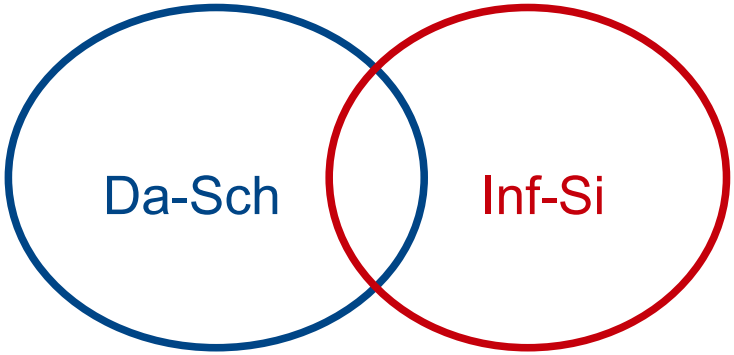
Verhältnis Datenschutz – Informationssicherheit ?



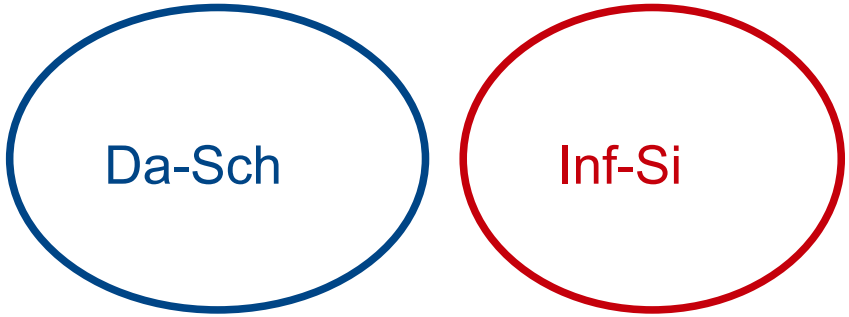
A



B



C

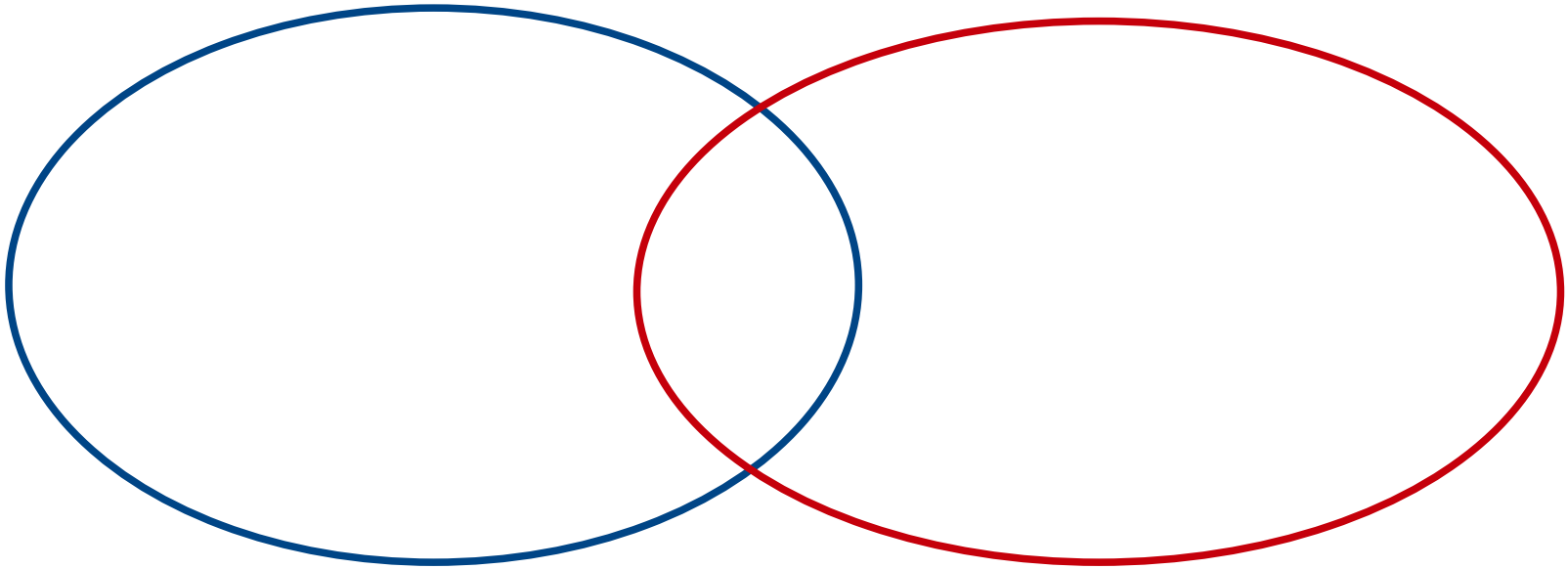


D

Abstimmung

- A
- B
- C
- D

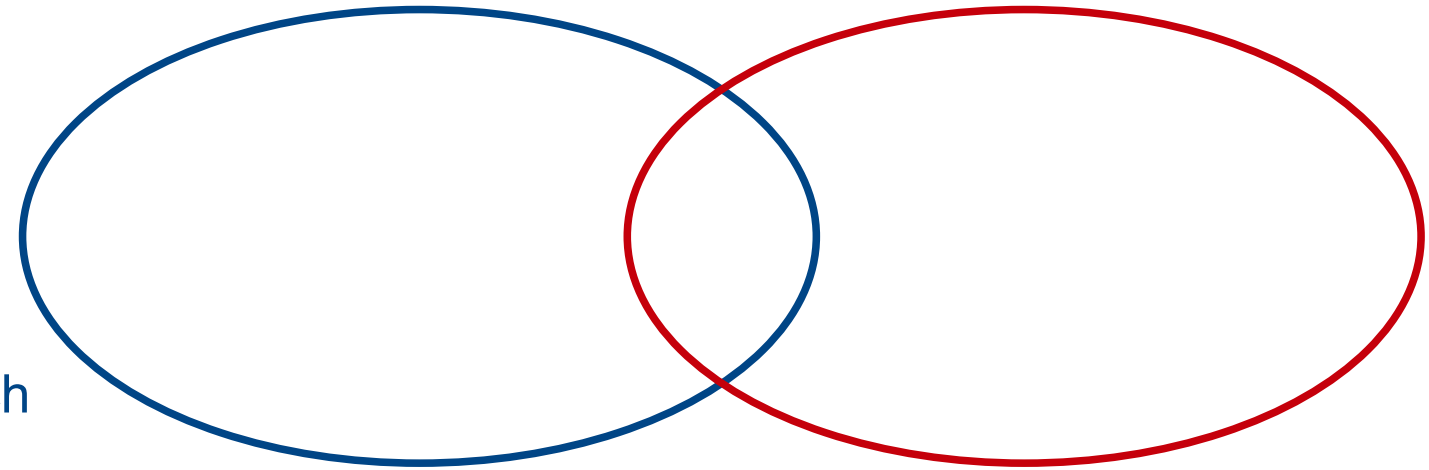
Verhältnis Datenschutz – Informationssicherheit ?



Da-Sch

Inf-Si

Verhältnis Datenschutz – Informationsicherheit ?



Da-Sch

Inf-Si

- Rechtsvorschriften zur Zulässigkeit der DV
- Meldepflichten
- Auskunftspflichten

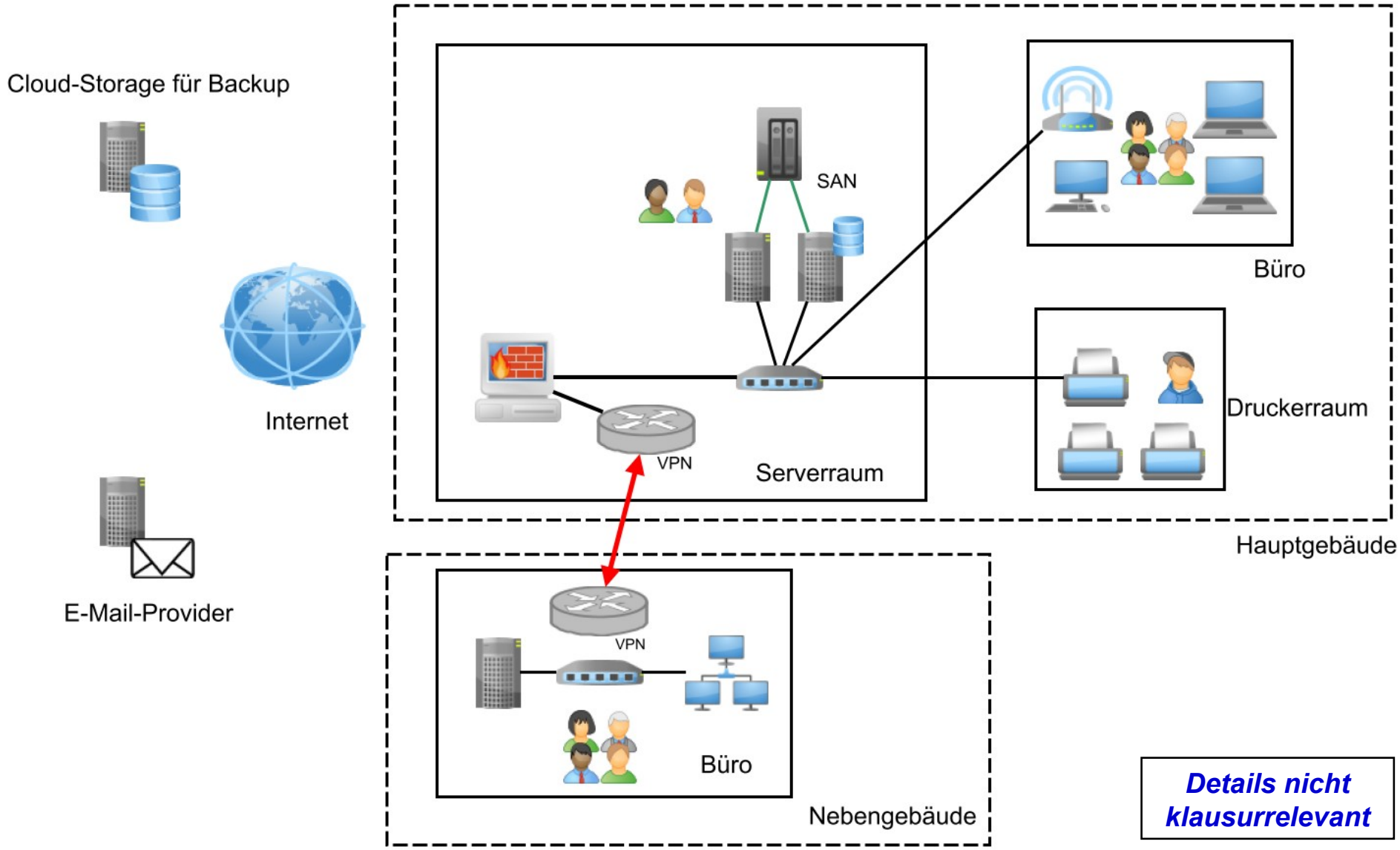
- Sicherheit personenbezogener Daten
- Protokollierungs-pflichten

- Sicherheit nicht-personenbezogener Daten (z. B. Betriebs-/Geschäftsgeheimnisse)
- häufig:Verfügbarkeit

Technisch-organsiatorische Maßnahmen

- Begriff des Bundesdatenschutzgesetzes/der DSGVO
- Maßnahmen, um die Ziele des Gesetzes zu erreichen
- Abwehrmaßnahmen („X soll nicht passieren“)
- Positive Maßnahmen („Y soll passieren“)

- Risikobegriff



Details nicht klausurrelevant

Aufgabe

Legen Sie geeignete Datenschutzmaßnahmen fest.
Legen Sie geeignete Sicherheitsmaßnahmen fest.

Diskussion: Was soll geschützt werden?

- Was soll Informationssicherheit erreichen?
- Schutz in Bezug auf was?
  (Richtigkeit der Daten? Finanzen? ...)

Systematik Zielvorgaben vs. Sicherheitsmaßnahmen

Unterschiedliche Detaillierungsgrade von Vorgaben

- in Gesetzen häufig sehr abstrakt
  - teilweise Zielvorgaben: „ Vertraulichkeit“
  - teilweise abstrakte Maßnahmenvorgaben: „Eingabekontrolle“
  - teilweise konkrete Maßnahmenvorgaben: „Verschlüsselung“

- in Branchen/Industriestandards häufig sehr ausführlich und konkret (z. B. „ TLS 1.3 -Verschlüsselung zwischen Clients und Server“)

Klassische Schutzziele (CIA)

- Vertraulichkeit (Confidentiality)
- Integrität (Integrity)
- Verfügbarkeit (Availability)

Vertraulichkeit

Vertraulichkeit: Informationen dürfen nur Berechtigten bekannt werden.

- Schutz von Vertraulichkeit:
  Verhindern von unberechtigter Kenntnisnahme,
- z.B. durch
  - Verschlüsselung von Daten (Kryptographie)
  - Verstecken von Daten (Steganographie)
  - Verhindern des Zugriffs auf Daten (Zugriffskontrolle)

```
-----BEGIN PGP-----
0IxWZHhKYoECwCBeIweKU+0Ed
m068SB4ADeGGCtd+eacjDT5Ig
TdwAypl8+WOFYxTVEXbqOqjoW
mY4T9zuoSC5e
=lu9g
-----END PGP-----
```

Wer darf unter welchen Bedingungen welche Daten lesen?

Grundsatz:

Die Verletzung der Vertraulichkeit personenbezogener Daten kann nicht ungeschehen gemacht werden.

Ein verratenes Geheimnis ist keines mehr und wird nie wieder eines!

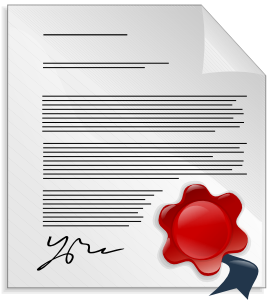
Integrität

Integrität: Informationen sind richtig, vollständig und aktuell
oder aber dies ist erkennbar nicht der Fall.

Schutz von Integrität:

Verhindern von unberechtigter Manipulation oder Datenverlust , z.B. durch

- Prüfsummen, fehlerkorrigierende Codes
- Einschränkung von Schreibrechten
- Erkennen von Manipulationen durch
  - Zeitstempel
  - Protokolle
  - Signaturen und Prüfsummen



www.openclipart.org

Wer darf unter welchen Bedingungen welche Daten oder IT-Systeme ändern?

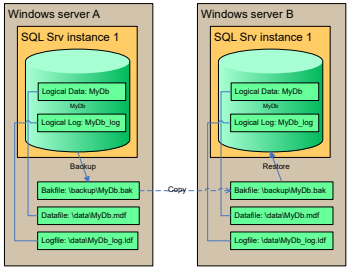
Verfügbarkeit

Verfügbarkeit: Informationen sind dort und dann zugänglich, wo und wann sie von Berechtigten gebraucht werden.

Schutz von Verfügbarkeit:

Gewährleisten von Funktionalität gegen vorsätzliche oder versehentliche Einschränkung, z.B. durch

- Redundanz (Daten, Hardware)
- Wartung
- Sicherheitsmaßnahmen (z. B. Firewall)



www.openclipart.org

Bedrohungen der Verfügbarkeit

Beispiele:

- E-Mail-SPAM
- DDOS (Distributed Denial of Service)
- Sabotage: **Ransomware**

- Feuer, Rauch
- Hardware-Versagen (z.B. Speicher, Switches, Netzteil, interne Kühlung)
- Infrastrukturausfall: Strom, Kühlung, Netze
- Infrastrukturausfall: Gebäudeschäden, Wasserschaden, Erdbeben
- Infrastruktur-Sabotage

- bei Dienstleistungen: Vertragsuntreue, „Kill Switch“

Sicherheitsvorfälle

Finden Sie Beispiele für

- (IT-)Sicherheitsvorfälle
- Datenschutzvorfälle

Heise 21.10.2023
https://heise.de/-9318038

Vor einigen Monaten ist es der Ransomware-Gang Clop gelungen, eine **Zero-Day-Lücke** in der **Datenaustauschsoftware MOVEit** auszunutzen. So konnten sie Daten aus dem Zugriffsbereich der Software-Nutzer stehlen. MOVEit wird weltweit von vielen Organisationen, Unternehmen und Dienstleistern zum Datenaustausch genutzt – dabei werden auch Daten **anderer Stellen und (Privat-)Personen** verarbeitet, die nicht in direktem Zusammenhang mit den Nutzern der Software stehen müssen.

Heise 10.12.2021
https://www.heise.de/-6291653.html

Über eine kritische **Zero-Day-Sicherheitslücke namens Log4Shell** in der weitverbreiteten Java-Logging-Bibliothek Log4j können Angreifer beliebigen Code ausführen lassen. Betroffen sind etwa Dienste von Apple, Twitter, Steam, Amazon und vermutlich sehr viele kleinere Angebote. Es gibt Proof-of-Concept-Code, der das Ausnutzen der Lücke demonstriert und auch bereits erste Angriffe. Seit Kurzem steht ein Quellcode-Update des Apache-Projekts bereit; Admins sollten dringend aktiv werden….

Heise 23.3.2024
https://www.heise.de/-9662578.html

Datenleck bei beliebter KiTa-App XXX

Bei der App "XXX", die in über **11.000 Kitas**, Horten & Schulen zum Einsatz kommt, gab es ein Datenleck. Potenziell betroffen sind über **800.000 Nutzer**. …

Der Server ... lieferte direkt ein "**Directory Listing**" seines Inhalts. ... liegen auf einem Server Dateien, die nicht für die Öffentlichkeit bestimmt sind, offenbart Directory Listing sie gnadenlos. Das eigentliche Problem im konkreten Fall ist aber der **fehlende Zugriffsschutz** auf die Dateien…..

Unter den ungeschützten Daten befanden sich fast 1500 CSV-Dateien, die jeweils persönliche Daten einer Vielzahl von Personen enthielten, insbesondere von Minderjährigen. In Verbindung mit **Namen, Geburtsdaten und Anschriften** fanden sich teilweise auch **Herkunftsländer, Informationen über Impfungen, Konfessionen, Erziehungsberechtigte, Notfallkontakte**, Klassenlehrer und vieles mehr.

Heise 04.09.2024 https://heise.de/-9857069

Seit Anfang September sind die IT-Systeme der XXXkliniken in ... lahmgelegt. ... Demnach ist der Klinikbetrieb durch den Ausfall der Serversysteme **massiv eingeschränkt** und auf eine analoge Notfallstruktur umgestellt worden. Geplante Operationen wurden abgesagt, weitere Absagen könnten folgen.

…. **Unklar** ist bislang, ob die Täter ein Lösegeld fordern oder **sensible Daten gestohlen** haben. Erste Maßnahmen zur Sicherung und Analyse der Daten wurden umgehend eingeleitet. "Von dem Angriff auf die IT betroffen sind nach einer ersten Analyse Verschlüsselungen virtueller Server im Krankenhaus-Informationssystem", heißt es im Bericht.

https://en.wikipedia.org/wiki/Heartbleed
(Abruf 27.04.2026)

Implementierungsfehler in Open SSL (2012-2014)

Heartbleed is a security bug in some outdated versions of the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. It was introduced into the software in 2012 and publicly disclosed in April 2014.

Heise 27.04.2026
https://www.heise.de/-11272997.html

Gesundheitsdaten der **UK Biobank** wurden online angeboten. Der Zugriff ist inzwischen gestoppt. Weitere Sicherheitsmaßnahmen sind geplant.

Wie ..., Minister of State, erklärte, hatte die UK Biobank die Regierung bereits am 20. April darüber informiert, dass mehrere **Angebote auf Alibaba-Plattformen** entdeckt worden waren. „Die Biobank teilte uns mit, dass drei Angebote identifiziert worden seien, die offenbar Daten von Teilnehmern der UK Biobank zum Verkauf anbieten. Mindestens einer dieser drei Datensätze scheint Daten von allen **500.000 Freiwilligen** der UK Biobank zu enthalten“, heißt es ....

Bewertungsportal

„... hat eine vierstellige Geldbuße gegen einen Arzt verhängt. Der Patient einer Arztpraxis hatte sich über diese auf einem Bewertungsportal im Internet kritisch geäußert. Der Arzt reagierte darauf mit einem Gegenkommentar, wobei er personenbezogene Daten des Patienten - wie Diagnosen und Behandlungsergebnisse – veröffentlichte."

https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-arzt-2023-12-31-DE-3753.php

Krankheitstage im Betrieb

Der Personalbereich eines Unternehmen hatte bezüglich einer jährlichen Beurteilung eine Liste erstellt, in der Name und Krankheitstage von Beschäftigten vermerkt wurden. Diese Liste wurde per E-Mail an einen Verteiler mit **allen** höherrangigen Führungskräften geschickt. Letzteres verstoße gegen den Beschäftigtendatenschutz.

https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-textilunternehmen-2023-06-15-DE-2972.php

fehlende Vereinbarung für gemeinsame Datenverantwortlichkeit, unrechtmäßige Datenverarbeitung, keine Löschung

Der … erließ eine Strafe gegen ein Immobilienunternehmen. Dieses hatte

- keine Vereinbarungen über gemeinsame Datenverantwortlichkeit getroffen und hatte zudem
- Daten erhoben und verarbeitet, ohne dass es dafür eine rechtliche Grundlage gab.
- Löschungsanfragen von drei Betroffenen wurde nicht rechtzeitig nachgekommen.

https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-unternehmen-2024-06-06-DE-3847.php

Heise 27.04.2026
https://www.heise.de/-11272997.html

UK Biobank II

Zugänge gesperrt und Datenzugriff vorerst gestoppt

Nach Bekanntwerden des Vorfalls wurden mehrere Sofortmaßnahmen eingeleitet. Gemeinsam mit der UK Biobank, den Plattformbetreibern und chinesischen Behörden seien die Angebote zügig entfernt worden. ...

Darüber hinaus wurde der **Zugriff** auf die UK Biobank vorübergehend **pausiert.** Downloads sind derzeit gestoppt, bis technische Maßnahmen implementiert sind, die ein **unkontrolliertes Herunterladen** künftig **verhindern** sollen. Die Organisation hat sich zudem selbst bei der britischen Datenschutzaufsicht (ICO) gemeldet.

Datenschutzziele

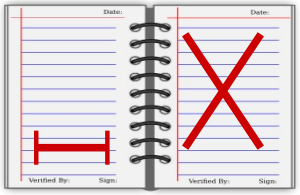
Sind diese Problemlagen durch die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität abgedeckt?

Formulierung weiterer Gewährleistungsziele

Datenminierung

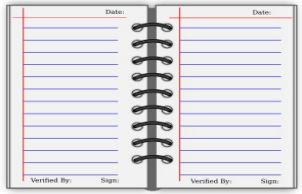
Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

- direkte Anforderung aus der DSGVO (Artikel 5)
- im Hinblick auf
  - Umfang,
  - Detaillierungsgrad,
  - Verarbeitungsdauer,
  - Speicherdauer,
  - Identifizierbarkeit



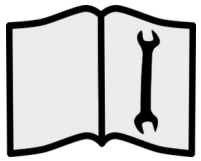
Transparenz

Die Datenverarbeitung ist für Betroffene nachvollziehbar und erfüllt prüfbar die datenschutzrechtlich bestehenden Anforderungen.



Sicherung von Transparenz:

- Dokumentation von Verfahren (Daten, IT-Systemen, technische Funktionen, organisatorischen Regelungen)
- (Teil-)Veröffentlichung gegenüber Betroffenen
- Protokollierung

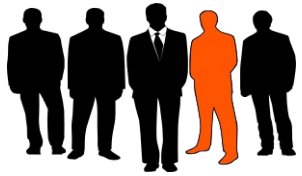


www.openclipart.org,

AI content by https://muryou-aigazou.com/

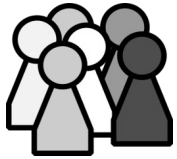
Nicht-Verkettung

Keine Zusammenführung personenbezogener Daten, die für verschiedene Zwecke verarbeitet werden.



Sicherung von Nicht-Verkettung z.B. durch

- Festlegung der Verfahrenszwecke
- Rollenkonzepte für Lesen/Schreiben/Löschen
- Trennung von Verfahren durch Trennung der Daten-bestände, IT-Systeme und Prozesse



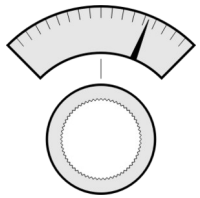
www.openclipart.org

Intervenierbarkeit

Betroffenenrechte müssen umsetzt werden können.
=> Verarbeitungen müssen verändert werden können.

Sicherung von Intervenierbarkeit:

- Changemanagement für Störungen, Problembearbeitungen und Änderungen einer Organisation
- Single Point of Contact für Betroffene
- Ausnahmebehandlung



www.openclipart.org

Spezifische Datenschutzschutzziele:

- Konkretisierung/Detaillierung von Anforderungen
- Formulierung als Gewährleistungsziele:[„Baue die Datenverarbeitung so, dass die gesetzlichen Vorgaben erfüllt werden können.“]

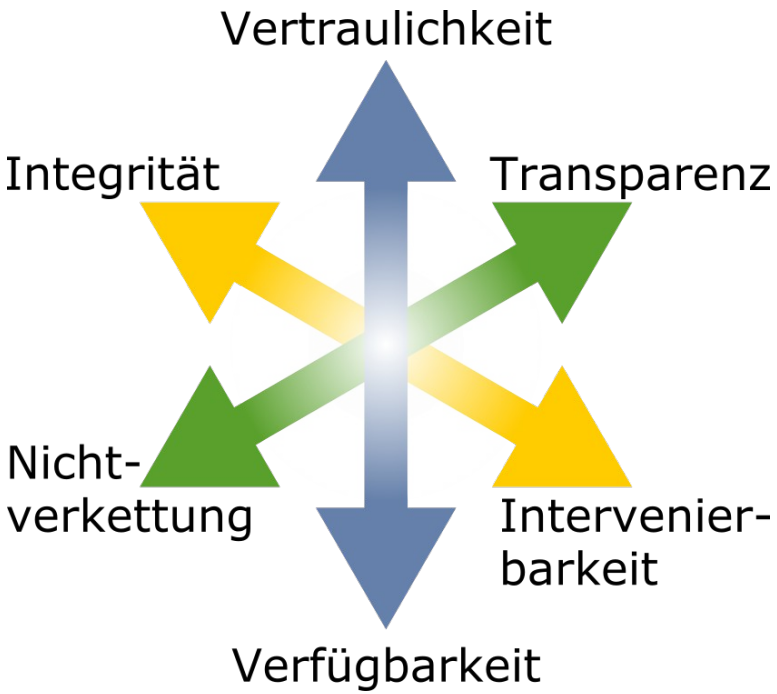
Gegensätzliche Schutzziele

Schutzziele können im Widerspruch stehen

- Vertraulichkeit vs. Verfügbarkeit
- Transparenz vs. Nichtverkettung
- Integrität vs. Intervenierbarkeit

Diskussion:

- Blockchain
- Cloud-Backup



Sicherheitsmanagement

Management is that for which there is no algorithm. Where there is an algorithm, it‘s administration.

- Roger Needham -

Zwei Fragestellungen:

- Welche Risiken/Bedrohungen sollen angegangen werden?
- Wie können sie angegangen werden?

Antwort:

- Risikomanagement
- **T**echnische und **O**rganisatorische (Sicherheits-)**M**aßnahmen (**TOM**)

Sicherheitsmanagement