



SENNESTADT GmbH
Stadtteilentwicklung seit 1956



Umsetzung der EU-DSGV und des neuen BDSG im Zeitalter von Big Data

FH Bielefeld
University of
Applied Sciences



Status Quo der Digitalisierung Big Data



komplex



allgegenwärtig

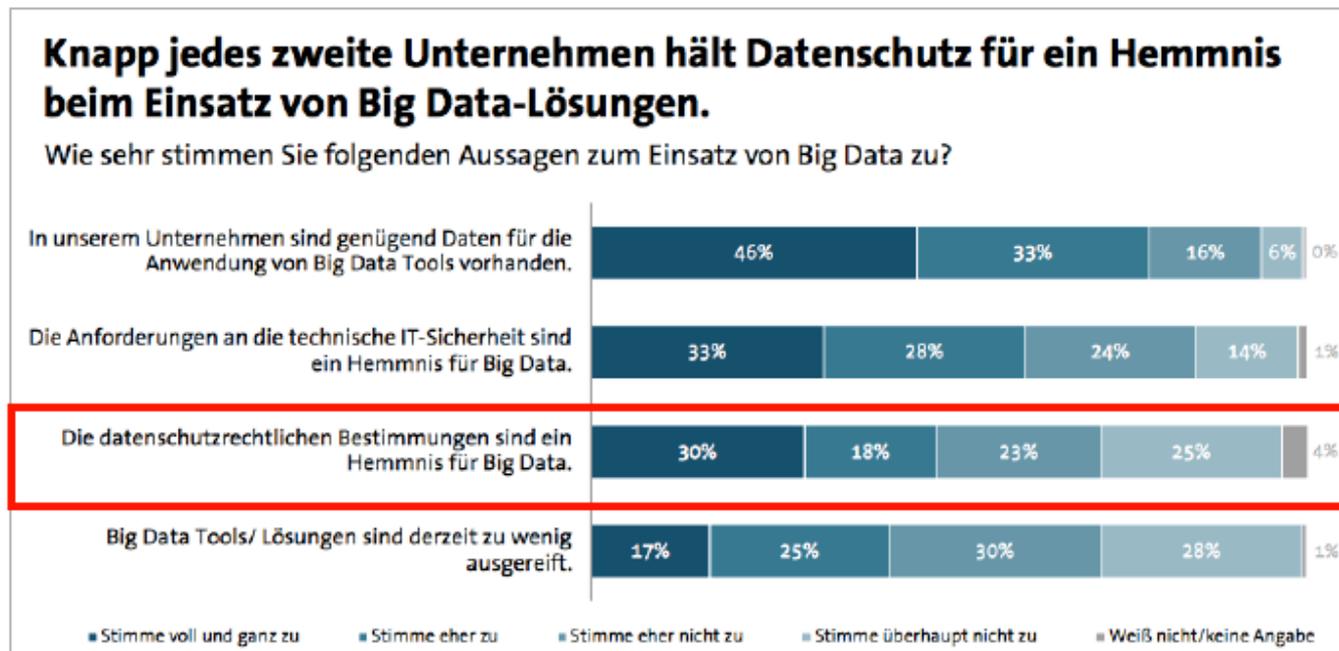
vernetzt



**Ich weiß, was Du gestern
getan hast ... und mit hoher
Wahrscheinlichkeit,
was Du morgen tun wirst.**



- orts- und raumbezogene Datenanalyse
- Text- und semantische Datenanalyse
- Video- und Audioanalyse
- Reporting
- Data Mining



Quelle: Bitkom 2017

Bahn akzeptiert Bußgeld für Datenskandal
1,1 Millionen Euro Strafe: Es ist die bislang höchste Bußgeldforderung einer deutschen Datenschutzbehörde – und die Deutsche Bahn hat in die Zahlung eingewilligt.
23. Oktober 2009

Ausland Neuer Datenskandal US-Polizei scannt Millionen Nummernschilder
Veröffentlicht am 18.07.2013

"Hello Barbie" gehackt: das Spielzeug als Überwachungs-Marionette
E-Mail-Verkehr und Internetnutzung
28.11.2015

17. Mai 2010, 21:05
Mitarbeiter-Bespitzelung
Auch Ikea und Burger King überwachten Personal
Die Bespitzelungsaffäre zieht immer weitere Kreise: Nun geraten zwei weitere Firmen unter Druck. Ikea und Burger King sollen ihre Mitarbeiter gefilmt haben.

Bespitzelung von Mitarbeitern
11.09.2008,

Lidl soll 1,5 Millionen Euro Bußgeld zahlen

Für Lidl wird die Bespitzelung von Mitarbeitern teuer:

Datenschützer mehrerer Bundesländer verlangen 1,5 Millionen Euro Bußgeld. Denn Angestellte in 2700 Filialen sollen systematisch überwacht worden sein - bis hin zu privaten Telefonaten und Gesprächen.

Datenskandal
Bahn spähte auch Krankheitsdaten aus
Datum: 04.08.2009

- Schutzobjekte und Schutzziele
- Informationssicherheit: Angemessener Schutz der Informationen (= Geschäftswerte / Assets) vor Bedrohungen



- Datenschutz: Schutz der Persönlichkeitsrechte
- Bundesverfassungsgericht zur Volkszählung:
 - Schutz des Einzelnen vor Beeinträchtigung seiner Persönlichkeitsrechte durch den Umgang mit seinen personenbezogenen Daten



Bundesdatenschutzgesetz (BDSG)

Regelt den Umgang mit personenbezogenen Daten, die nichts mit Kommunikation über Netzwerke zu tun haben, wie z. B. Passwortänderungen oder Dateizugriffe.



Telekommunikationsgesetz (TKG)

Schützt den Informationen auf dem Übertragungsweg und regelt den Umgang mit Daten, die Auskunft über die Nutzung der Kommunikationswege geben: Wer hat wann mit wem eine Netzwerkverbindung aufgebaut?



Telemediengesetz (TMG)

Regelt den Umgang mit Daten bei der Nutzung von Tele- und Mediendiensten: Wer hat welche Webseite oder andere Datendienste abgerufen?

- Sanktionen bei Verstößen:
 - § 43 Abs. 1 BDSG: z. B. gegen Meldepflichten
→ bis zu € 50.000,-
 - § 43 Abs. 2 BDSG: z. B. unbefugtes Erheben
→ bis zu € 300.000,-
- Ahndungen als Straftat: § 44 BDSG
- Sanktionen der Aufsichtsbehörden
(data protection authority):
 - Auskunft, Verhängung und Durchsetzung von Zwangsgeld.
 - Umsetzung von Maßnahmen zur Mängelbeseitigung
(Anordnung sämtliche Verstöße gegen Datenschutz zu beseitigen!).
 - Behörde kann Einsatz einzelner Verfahren nun untersagen!
 - Keine Beschränkung mehr nur auf Prüfung technischer Organisationsmaßnahmen. Beachte: Reputationsrisiko

- Jede Person hat Schadensersatz gegen den für die Verarbeitung Verantwortlichen oder gegen Auftragsverarbeiter
- Sanktionen der Aufsichtsbehörden bei Verstößen:
 - Bußgelder:
 - bis zu 2 % (von bis zu 10 Mio), z.B. Auftragsverarbeiter, DSB, etc.
 - bis zu 4 % (von bis zu 20 Mio), z.B. Einwilligung, Übermittlung des weltweiten Jahresumsatz des Unternehmens im vergangenen Geschäftsjahr
- nicht zu vergessen:
 - möglicherweise auch einen Straftat
 - personelle Konsequenzen: Abmahnung/Kündigung

Beachte: REPUTATION!



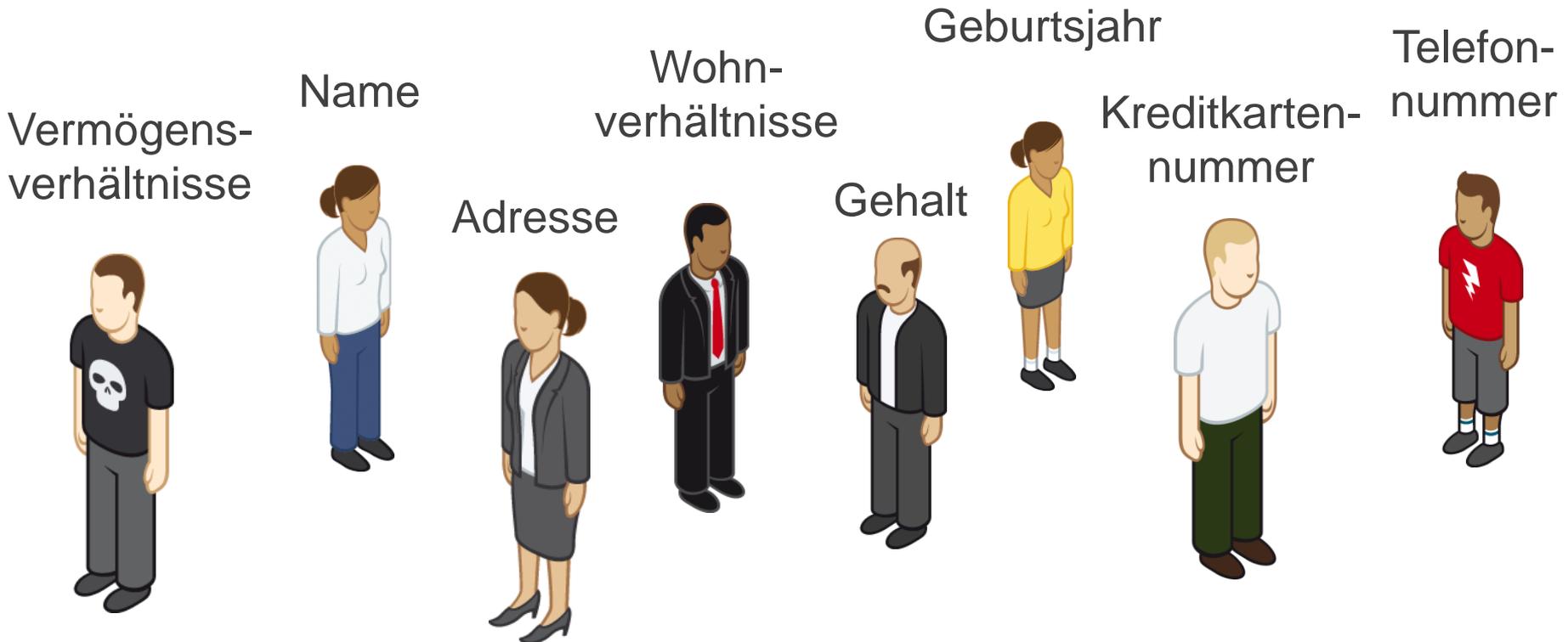
Wichtige neue Grundregelungen der EU-DSGVO im Überblick



- **Rechtsnatur** der DSGVO: Keine Auffanggesetz, Vorrangregelung
- **Globale** Anwendung der DSGVO: **Marktortprinzip**
- **Haftung** auch für immaterielle Schäden und für Auftragsverarbeiter
- **Risikobasierter** Datenschutz
- Erweiterte Pflichten für Unternehmen gerade bzgl. Aspekte der Dokumentations- und Nachweispflichten
- **Informationspflichten** bei Datenerhebung des Verantwortlichen
- **Datenschutz-Folgeabwägung** (statt Vorabkontrolle)
- Löschfristen und „Recht auf Vergessenwerden“
- Melde- und Benachrichtigungspflichten bei Verletzungen
- „**Privacy by design**“ und „**Privacy by default**“; Verpflichtung zur Umsetzung und Gewährleistung der Datensicherheit

Personenbezogene Daten sind alle Angaben, die sich auf eine bestimmte oder aber auch nur bestimmbare Person beziehen.

Beispiele:



Bestimmt ist eine Person, wenn sich ihre Identität direkt aus dem Datum selbst ergibt.

Bestimmbar wird eine Person, wenn ihre Identität durch die Kombination des Datums mit einer anderen Information feststellbar wird.



Weitaus strengere Regeln gibt es für den Umgang mit sogenannten **besonderen Arten personenbezogener Daten**, da diese besonders schützenswert sind.

Politische
Meinung



Gewerkschafts-
zugehörigkeit



Ethnische
Herkunft



Religiöse
Überzeugung



Gesundheit



Sexual-
leben



Das BDSG **verbietet** grundsätzlich die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, erlaubt diese aber unter bestimmten Voraussetzungen (Verbot mit Erlaubnisvorbehalt).

Datenerhebung ist somit zulässig, wenn sie ...



durch das BDSG selbst ...

Beispiel: öffentlich zugängliche Daten



oder durch eine andere Rechtsvorschrift ...

Beispiel: Steuern, Abgaben



oder durch die Einwilligung des Betroffenen ...

Beispiel: Einverständniserklärung zur Datennutzung

... erlaubt wird.

Grundsatz

Die Verwendung von personenbezogenen Daten ist verboten.

Ausnahmen

Erhebung, Verarbeitung und Nutzung personenbezogener Daten muss explizit erlaubt werden (Verbotsprinzip mit Erlaubnisvorbehalt)

Die Ausnahmen ergeben sich aus:

- BDSG: Bestehendes Arbeitsverhältnis (§ 32)
- Betriebsvereinbarungen (BV)
- Einwilligung des Betroffenen

Grundprinzipien Datenschutz

Rechtmäßigkeit

- BDSG, andere Rechtsvorschrift, Einwilligung
- Nutzung für Beschäftigungsverhältnis

Einwilligung

- Freiwilligkeit
- Informationen über Tragweite
- Schriftform

Zweckbindung

- Vorabinformation des Betroffenen
- Verwendung nur zum **originären Zweck**

Datensparsamkeit, -vermeidung, -löschung

- Keine überflüssigen Daten
- Nur so viele Daten wie nötig
- Löschung/Sperrung nach Zweckerfüllung/
Wegfall Geschäftsbedingung

Offene Datenerhebung (Transparenz)

- Datenerhebung direkt beim Betroffenen





EU-DSGVO: Beachtung der IT-Sicherheit



- IT-Sicherheit in der EU-DSGVO:
 - Implizite Pflicht zum IT-Sicherheitskonzept / IT-Sicherheitsmanagement
 - Pflicht zum Testen der Wirksamkeit
 - Sicherstellung der Verhinderung unbefugter Datenverarbeitung
 - (Erweiterte) Informations-/ Dokumentationspflichten bei Sicherheitsvorfällen; siehe Datenpanne

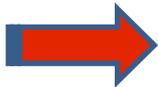
- Instrument der EU-Datenschutzgrundverordnung in Art. 35 DSGVO
- **Ähnlich:** Vorabkontrolle gemäß § 4 d Abs. 5, 6 BDSG



- **Vorgehensweise nach DSGVO**
 - Identifizieren und erste Bewertung der relevanten Risiken
 - Auswahl von technisch-organisatorischen Maßnahmen
 - Feststellung von verbleibenden Risiken und deren (End-) Behandlung
 - Data Protection Impact Assessments (DPIA) soll vorgeschrieben werden bei Videoüberwachung und Persönlichkeitsrechten

- Verantwortung der ordnungsgemäßen Verarbeitung bleibt beim Auftraggeber, § 11 Abs.1 BDSG
- ADV fordert schriftliche Vereinbarung zum:
 - Umfang der Datenverarbeitung
 - Datenschutz und Datensicherheitsmaßnahmen
 - Weisungsbefugnis und Kontrollen des Auftraggebers
 - Weitergabe der Daten vom Auftraggeber zum Auftragnehmer

Merke:



Auftragsdatenverarbeitung ist keine Übermittlung im datenschutzrechtlichen Sinne (sondern rechtliche Einheit!)

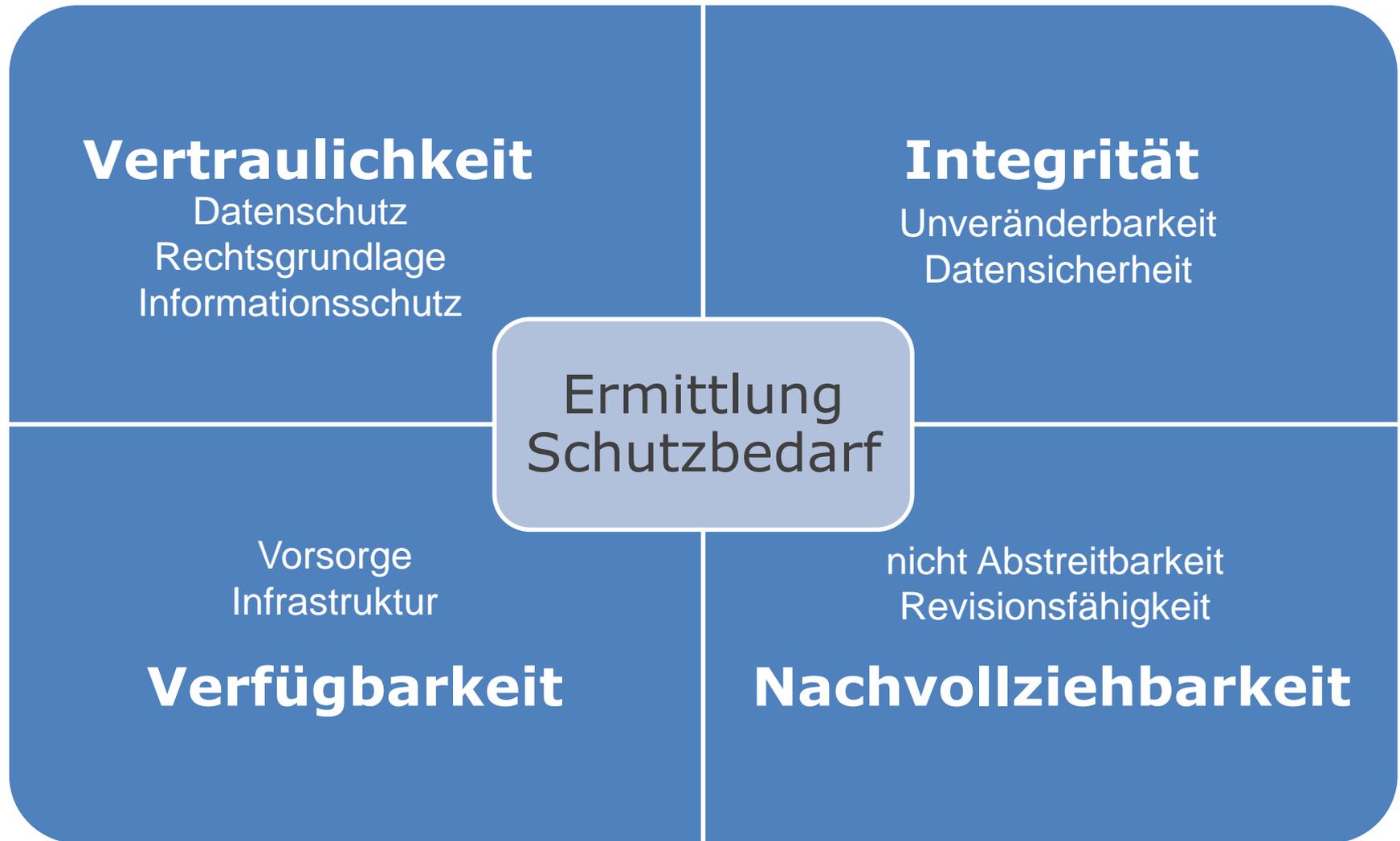
- ADV kann jedenfalls nur dann angenommen werden, wenn die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten angesehen werden kann als
→ „Hilfs- oder Unterstützungsfunktion“
- ADV kann durch weisungsgebundenen Dienstleister erbracht werden:
 - EDV-technische Teil der Lohn- und Gehaltsrechnung
 - Finanzbuchhaltung
 - Webadressenverwaltung
 - Betrieb eines Callcenters
 - E-Mail-Verwaltung
 - Datenverwaltung für den Betreiber von Internetseiten (Webhosting)
 - Speicherung von Backup-Sicherungsdatenbeständen
 - Datenträgervernichtung

- EU-Datenschutz-Richtlinie, mit dem Ziel ein einheitliches Schutzniveau innerhalb der Mitgliedstaaten sicherzustellen. In anderen Fällen muss eine Zwei-Stufen-Prüfung erfolgen:
- Bei Dienstleistern außerhalb der EU ist festzustellen:
 - 1) Ist Übermittlung an andere Unternehmen gemäß §§ 4, 28, ggfs. 32 BDSG zulässig?
 - ggfs. ohne Einwilligung
 - mit Einwilligung
 - Betriebsvereinbarung
 - 2) Ausreichendes und angemessenes Schutzniveau beim Unternehmen im Drittstaat?
 - Positiv-Liste
 - Früher: Safe Harbour, jetzt: Privacy Shield
 - Einsatz von EU-Standardvertragsklauseln



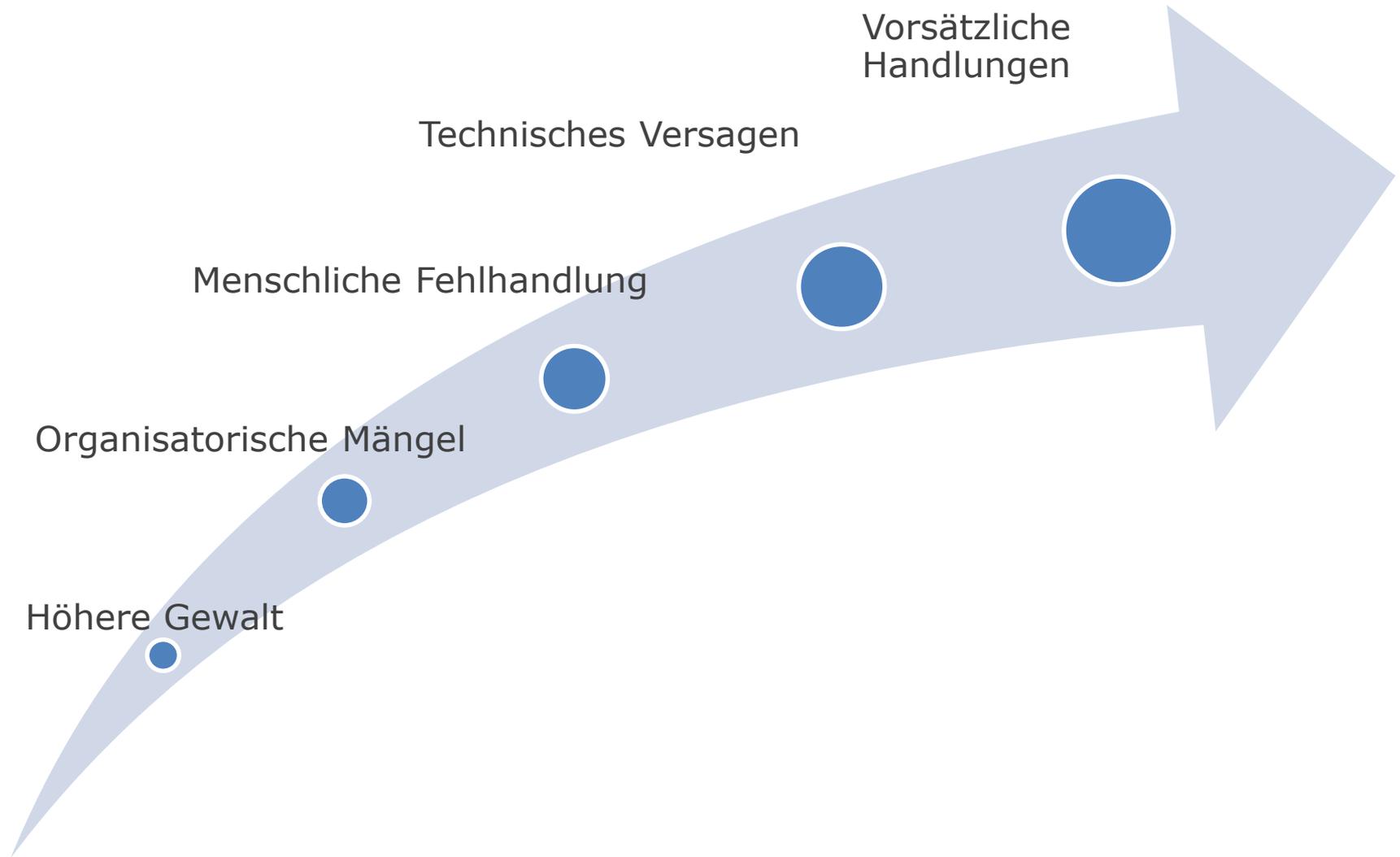
Datenschutz durch Datensicherung







Einige Gefahren / Risiken und Ziele der IT-Sicherheit



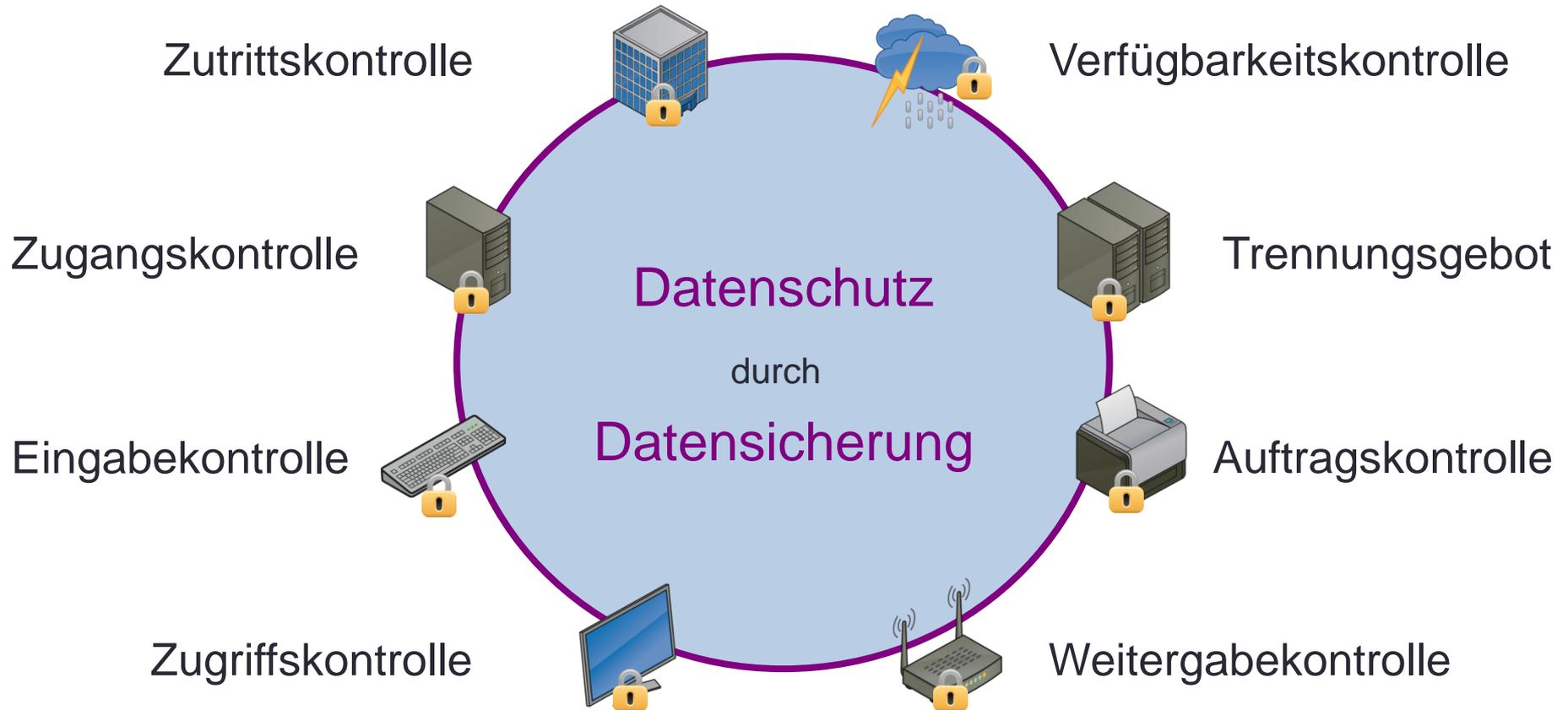
Höhere Gewalt

Organisatorische Mängel

Menschliche Fehlhandlung

Technisches Versagen

Vorsätzliche Handlungen



- Weitere Schutzziele des Datenschutzes
(z. B. § 10 Abs. 2 DSGVO NRW)

➔ Ziele Datensicherheit

- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Authentizität

+ Erweiterung

- Transparenz
- Revisionsfähigkeit
- Nichtverkettbarkeit
- Intervenierbarkeit

Nach Art. 32 (Sicherheit der Verarbeitung) DSGVO neben ToMs:

- Spezielle Vorgaben (Verschlüsselung, Notfallkonzepte, Pseudonymisierung etc.)
- Beschreibung inklusive Risikobewertung
- Regelmäßige Auditierung erforderlich

- Neue Gesetzgebung im Datenschutzbereich mit
 - dramatisch höheren Sanktionen bei Verstößen und
 - deutlich komplexeren Anforderungen an die Umsetzung (Risikobasierter Ansatz)
- Anforderungen an die Sicherheit und das Design („**Privacy by design**“ und „**Privacy by default**“)
- bereits im Entwurf und der Planung von Lösungen und Systemen berücksichtigt