

# Datenschutz & Datensicherheit

Franz Hoheiser-Pförtner

# Bewusstsein für Datenschutz & Informationssicherheit fördern

*“Ein gemeinsames Verständnis der Herausforderungen ist die zentrale Voraussetzung, um Maßnahmen zur Verbesserung des Datenschutzes und der Informationssicherheit bei E-Health Anwendungen zu verstehen bzw. diese zu fördern”*

# Ein Statement für Informationssicherheit im Gesundheits- & Sozialwesen

*“Die Sicherheitsanforderungen, die sich die Gesundheitsdiensteanbieter bei E-Health Anwendungen auferlegen beruhen einerseits auf einem hohen Verantwortungsempfinden und auf der Tatsache, dass die Gesundheitsdiensteanbieter täglich für Leib und Leben von vielen Menschen mitverantwortlich sind und anderseits auf verbindlichen Rechtsvorschriften zur Informationssicherheit bzw. im Umgang mit sensiblen und damit besonders schützenswerten Daten”*

# **DATENSCHUTZ ist Datenvermeidung & Datensparsamkeit**

*„Privacy by Design and Default“*  
oder  
Datenschutz durch Technikgestaltung und  
datenschutzfreundliche Voreinstellungen

# Zwecke des Datenschutzes 1/4

Schutzgut sind nicht die Daten selbst, sondern verschiedene grundrechtlich geschützte Sphären der Menschen, über die Informationen verarbeitet werden

- z.B. Privatsphäre, Opferschutz, Antidiskriminierung, faires Verfahren, geheimes Wahlrecht,...

# Zwecke des Datenschutzes 2/4

Nur wenige Grundrechte gelten vorbehaltslos –  
Eingriff z.B. durch gesetzliche Auskunftspflichten von  
Telekomanbieter an Sicherheitsbehörden

# Zwecke des Datenschutzes 3/4

„Wer nichts zu verbergen hat, hat auch nichts zu befürchten“?

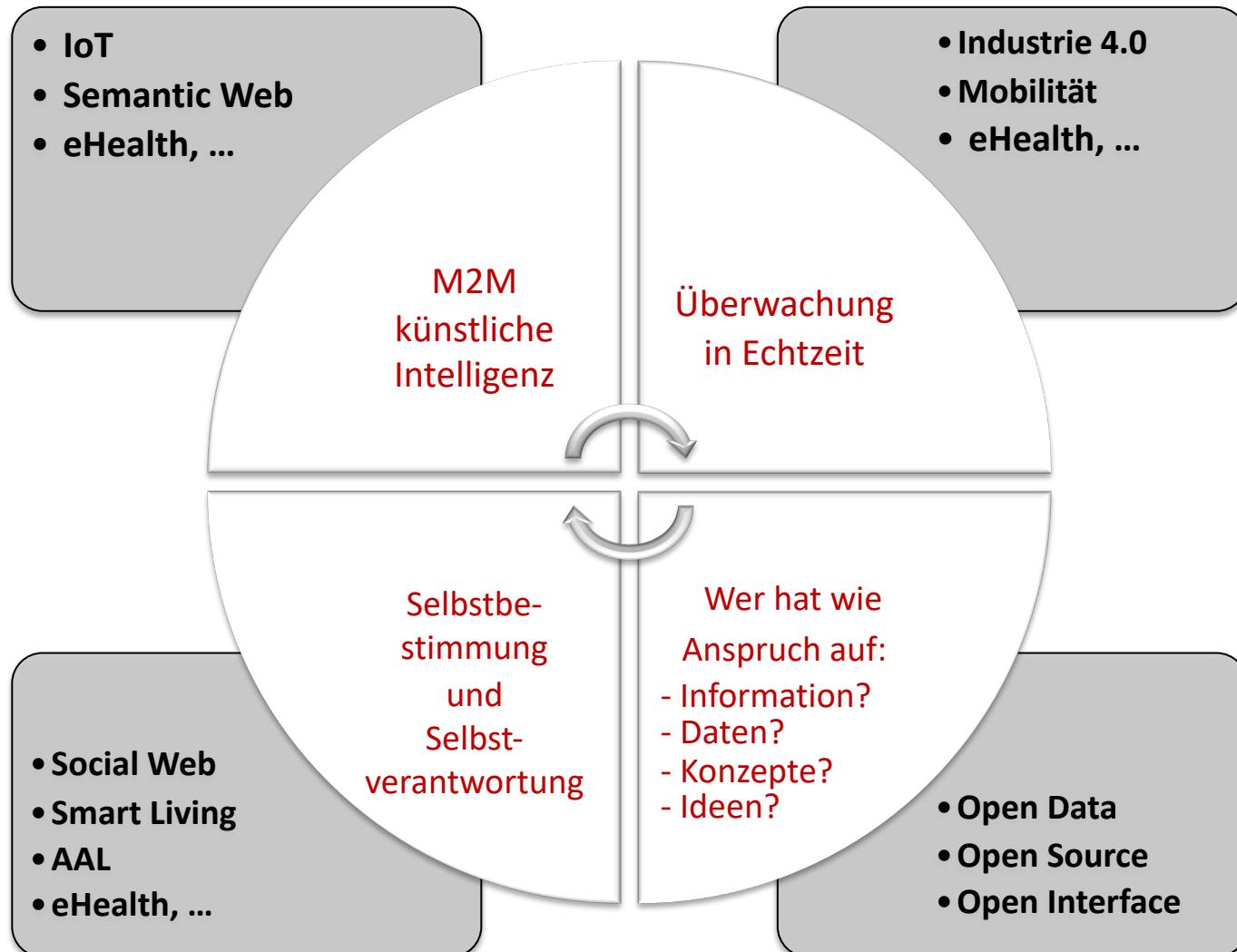
- Umkehrung der Rechtfertigungslast verletzt liberales Prinzip der Verfassung
- Stärkung des Menschenrechtsbewusstseins

# Zwecke des Datenschutzes 4/4

Die Frage der  
„Digitalen Menschenrechte“  
geht über Datenschutz hinaus:

- Online-Versammlungsfreiheit, Online-Meinungsfreiheit,  
Recht auf Netzzugang, Netzneutralität,...

# Anwendungsfelder



# Anwendungsoptionen

## lt. EU-DSVG

- Semantic Web
- eHealth, ...

- Industrie 4.0
- Mobilität
- eHealth, ...

... interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik „**data protection by design**“ und durch datenschutzfreundliche Voreinstellungen „**data protection by default**“ Genüge tun...

... die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich **pseudonymisiert** werden, **Transparenz** in Bezug auf die Funktionen und die **Verarbeitung personenbezogener Daten** hergestellt wird, ...

# Abgrenzung Datenschutz & Datensicherheit



# 10 Datenschutzregeln / -kontrollen

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen (personenbezogene) Daten verarbeitet werden, zu verwehren
- **Zugangskontrolle**
  - Sicherheitsschloss,
  - abschließen der Räume,
  - Schlüsselbuch,
  - nicht einsehbare Aufstellung von Geräten,
  - Überwachungs- und Alarmanlagen, ...

# 10 Datenschutzregeln / -kontrollen

2. zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können
- **Datenträgerkontrolle**
    - spezielle Räume zur Aufbewahrung
    - Datensafe,
    - Bestandskontrollen,
    - kontrollierte Vernichtung, ...

# 10 Datenschutzregeln / -kontrollen

3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern
- **Speicherkontrolle**
  - Trennung von Daten- und Programmbereichen verschiedener Benutzer(gruppen),
  - Verschlüsselung, ...

# 10 Datenschutzregeln / -kontrollen

4. zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zu Datenübertragung von Unbefugten genutzt werden können
- **Nutzerkontrolle**
    - Passwortregelungen,
    - sonstige Identifikationsverfahren,
    - Identitätsmanagement (IdM) ...

# 10 Datenschutzregeln / -kontrollen

5. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können
- **Zugriffskontrolle**
    - Berechtigungskonzepte,
    - Berechtigungstechnik (MAC, DAC, RBAC, ...),
    - Protokollierung von Zugriffen,
    - zeitliche Begrenzung von Zugriffen,
    - revisionsfähige Dokumentation der Benutzerprofile, ...

# 10 Datenschutzregeln / -kontrollen

6. zu gewährleisten, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können
- **Übermittlungskontrolle**
    - Definition von Sender, Empfänger und Art der zu übermittelnden Daten,
    - Dokumentation wer, wann, was,
    - Verschlüsselung, ...

## 10 Datenschutzregeln / -kontrollen

7. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind
- **Eingabekontrolle**
  - manipulationssichere Protokollierung,
  - Plausibilitätsprüfung, ...

# 10 Datenschutzregeln / -kontrollen

8. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Anweisungen des Auftraggebers verarbeitet werden können
- **Auftragskontrolle**
    - Protokoll über Auftrag und Erledigung,
    - eindeutige Vertragsgestaltung,
    - Unterweisungen, ...

# 10 Datenschutzregeln / -kontrollen

9. zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können
  - **Transportkontrolle**
    - Festlegung von Boten und Transportwegen,
    - Quittung,
    - Transportkoffer,
    - Verschlüsselung,
    - Authentifizierung, ...

# 10 Datenschutzregeln / -kontrollen

10. die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird

- **Organisationskontrolle**

- Verantwortlichkeiten festlegen,
- Verpflichtungen und Anweisungen,
- Verfahrens-, Dokumentations- und Projektrichtlinien
- Funktionstrennung - *Separation of duties* (SoD), ...

# Begriffe nach DIN 44300-1

- Datensicherheit
  - Sachlage, bei der Daten unmittelbar oder mittelbar so weit wie möglich vor Beeinträchtigungen und Missbrauch bewahrt sind
- Datensicherung
  - Maßnahmen und Einrichtungen, die Datensicherheit herbeiführen oder erhalten

- I. Datenschutz Grundlagen
- II. EU Datenschutzreform im Überblick
- III. DSGVO Compliance als Organisationsprojekt
- IV. Datenschutz nach DSGVO

Quelle: Ing. Mag. Dr. iur. Christof Tschohl

# Datenschutz-Grundlagen

- ✓ **Datenschutz ist ein Grundrecht:**
  - Art 8 Charta der Grundrechte der EU (GRC)
  - Art 8 Europäische Menschenrechtskonvention (EMRK)
  - § 1 DSG 2000 im Verfassungsrang
- ✓ **Datenschutz ist nicht Selbstzweck, sondern Voraussetzung für**
  - das Funktionieren einer freien demokratischen Gesellschaft und
  - die Ausübung zahlreicher anderer Grundrechte
- ✓ **Personenbezogene Daten:** Daten, die sich auf eine bestimmte oder bestimmbare natürliche Personen beziehen
- ✓ Verarbeitung personenbezogener Daten verboten, wenn nicht ausdrücklich erlaubt

## Das Grundrecht auf Datenschutz nach Art 8 EU Grundrechte-Charta

### ✓ Art 8 GRC:

Schutz personenbezogener Daten

- (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
- (2) Diese Daten dürfen nur nach **Treu und Glauben für festgelegte Zwecke** und mit **Einwilligung** der betroffenen Person **oder** auf einer sonstigen **gesetzlich geregelten legitimen Grundlage** verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die **Berichtigung** der Daten zu erwirken.
- (3) Die **Einhaltung dieser Vorschriften** wird von einer **unabhängigen Stelle überwacht**.

✓ Existiert eigenständig neben Art 7 GRC (**Schutz des Privat- und Familienlebens**)

✓ Zusammenhang mit Art 8 EMRK

- Art 52 GRC: Tragweite der Rechte wie EMRK nach Rechtsprechung des EGMR
- Rechtsprechung des EGMR zu Datenschutz aus Art 8 EMRK beachtlich!

## Grundrecht auf Datenschutz Schutzgarantien

- ✓ Umfasst Recht auf
  - Geheimhaltung
  - Auskunftserteilung
  - Richtigstellung und Löschung
  - Information über Datenverwendung
- ✓ personenbezogener Daten (nach DSGVO kein Schutz juristischer Personen)
- ✓ jeder Eingriff bedarf einer Rechtsgrundlage (Gesetz, Vertrag, Einwilligung oder Interessenabwägung)
- ✓ strenger Maßstab für besonders schutzwürdige („sensible) Daten“

## Datenschutz-Grundlagen besonders schutzwürdige Daten

- ✓ Noch strengere Beschränkungen für besondere Kategorien von Daten („sensible Daten“):
  - rassische und ethnische Herkunft
  - politische Meinungen
  - religiöse oder weltanschauliche Überzeugungen
  - Gewerkschaftszugehörigkeit
  - genetischen Daten
  - biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person
  - Gesundheitsdaten
  - Daten zum Sexualleben oder der sexuellen Orientierung

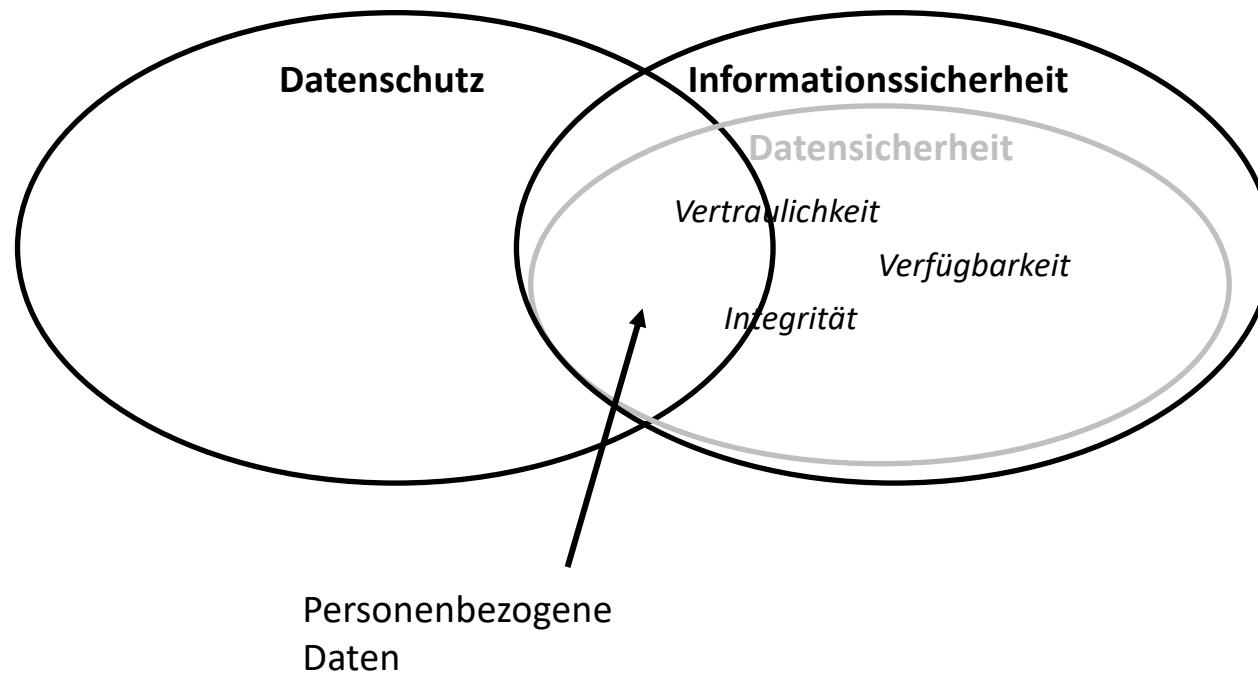
## Grundsatz der Zweckbindung und Verhältnismäßigkeit

### ✓ Immer beachtlich: **Grundsatz der Verhältnismäßigkeit**

Auch im Falle zulässiger Beschränkungen darf ein Eingriff in das Grundrecht jeweils nur in der gelindesten zum Ziel führenden Art vorgenommen werden.

- ✓ Ist die Verarbeitung ein Eingriff in die informationelle Selbstbestimmung?
- ✓ Ist der Eingriff gesetzlich vorgesehen und hinreichend bestimmt?
  - Für Private: wenn keine gesetzl. Grundlage dann eine vertragliche
- ✓ Dient der Eingriff einem legitimen Ziel?
  - Für staatliche Behörden: Aufzählung in Art 8/2 EMRK relevant
- ✓ Ist die Verarbeitung abstrakt geeignet, den Zweck zu erreichen?
- ✓ Gibt es gelindere Mittel, den Zweck zu erreichen?
- ✓ Angemessenem Verhältnis zwischen nachteiligen Konsequenzen und Nutzen?
  - ✓ Verhältnismäßigkeit erfordert auch wirksame kontroll- und Rechtsschutzinstrumente

# Datenschutz und Informationssicherheit



- I. Datenschutz Grundlagen
- II. EU Datenschutzreform im Überblick
- III. DSGVO Compliance als Organisationsprojekt
- IV. Datenschutz nach DSGVO

Quelle: Ing. Mag. Dr. iur. Christof Tschohl

# EU-Datenschutzreform: Ergebnis und Status Quo

- ✓ **Bisher:**
  - EU: Datenschutzrichtlinie, RL 95/46/EG
  - Österreichisches Datenschutzgesetz 2000 (DSG 2000)
- ✓ **Datenschutz-Grundverordnung (DSGVO), VO 2016/679**
  - Seit 24. Mai 2016 im Rechtsbestand der EU; wirksam ab 25. Mai 2018
  - Datenschutzrichtlinie tritt mit 25. Mai 2018 außer Kraft
  - Ziele und Grundsätze der DSRL gelten in der DSGVO fort
- ✓ **Entwurf der EU-Kommission für eine E-Privacy-Verordnung (17.1.2017)**
  - Sollte ebenfalls mit 25. Mai 2018 wirksam werden (mittlerweile äußerst unwahrscheinlich)
  - Spezialregelung für den Datenschutz im Bereich der elektronischen Kommunikation
  - bildet gemeinsam mit der DSGVO den datenschutzrechtlichen Rahmen der EU
- ✓ **Datenschutzrichtlinie für Polizei und Strafjustiz (DSRL-PJ), RL 2016/680**
  - Erstmals einheitlicher Datenschutzrahmen für Strafverfolgung und Gefahrenabwehr (auch rein innerstaatliche Datenverarbeitung)
  - Seit 5. Mai 2016 in Kraft; von den Mitgliedstaaten bis 6. Mai 2018 umzusetzen
- ✓ **Nationales Begleitgesetz: Umfassende Änderung des Datenschutzgesetzes (DSG) inkl. Umsetzung der DSRL-PJ am 31. Juli 2017 kundgemacht, BGBI I 2017/120**
- ✓ **Künftig: DSGVO-Auslegung durch EU-Datenschutzausschuss (Leitlinien, Empfehlungen etc.)**

## Rechtliche Anpassungen in Österreich

- ✓ **Keine „Umsetzung“ im engeren Sinn notwendig:** DSGVO ist eine EU Verordnung und bedarf keiner Umsetzung in nationales Recht → **unmittelbare Wirksamkeit**
- ✓ **Begleitgesetzgebung:** DSGVO enthält 30 explizite und viele implizite „Öffnungsklauseln“
  - Insb. „Flexibilisierungsklausel“ für den öffentlichen Sektor in Art 6 Abs. 2 DSGVO
  - Spielraum für nationale Gesetzgeber (Kritik: zu unspezifisch, keine Harmonisierung)
- ✓ **Zukünftiges nationales Datenschutzrecht in Österreich:** Nationales Begleitgesetz: Umfassende Änderung des Datenschutzgesetzes (DSG) inkl. Umsetzung der DSRL-PJ am 31. Juli 2017 kundgemacht, BGBl I 2017/120, enthält u.a.
  - Zuständigkeiten der Datenschutzbehörde
  - anzuwendendes Verfahrensrecht
  - subsidiäre Verwaltungsstrafen
- ✓ **Öffnungsklauseln (fast) nur für den öffentlichen Bereich ausdrücklich geregelt:**
  - die ausdrücklichen Öffnungsklauseln klammern weitgehend private Datenanwendungen aus (zB Videoüberwachung) → aber: Interpretativ iZm Erwägungsgrund 10
  - An vielen Stellen setzt DSGVO aber einen nationalen Rechtsbestand voraus

## Grundverordnung und Richtlinie als Gesamtpaket



## Wesentliche Neuerungen der DSGVO

### Verschärfung der Sanktionsmechanismen

- Öffentlich-rechtliche Haftung: Strafzahlungen bis 20 Millionen EUR oder 4 Prozent des weltweiten Jahresumsatzes des betroffenen Unternehmens
- Auch für Verletzung von Handlungspflichten, nicht nur bei Data Breach
- Verbandsklagen zulässig
- Datenschutzbehörde wird Strafbehörde

### Eigenverantwortung der „Verantwortlichen“ („Auftraggeber“)

- Dokumentationspflichten
- Rechenschaftspflicht
- Risikobasierter Ansatz
- Verpflichtende Risikoanalysen und Folgenabschätzung
- Datenschutzbeauftragter (in bestimmten Fällen)

### Datenschutz-Grundverordnung (DSGVO)

### Materiell-rechtliche Änderungen, zB

- Allgemeine “Data Breach Notification”
- Privacy by Design und by Default
- Entfall der Melde- und Genehmigungspflicht (DVR)
- Kein Schutz juristischer Personen mehr
- Wegfall der „indirekt personenbezogenen Daten“
- Recht auf Datenportabilität

### Verstärkte Kooperation der nationalen Datenschutzbehörden

- „One-Stop-Shop“-Prinzip für Betroffene
- neues Gremium "European Data Protection Board" (bisher: Art.-29-Gruppe)
- Konsultationsverfahren bei komplexen Risiken
- Mehr Koordination und Kohärenz

## Geldbußen (Art 83 DSGVO)

Hohe Strafandrohungen

- **Bis zu 20 Mio Euro oder 4 % des weltweiten Konzern-Jahresumsatzes**
  - **Verletzung von Betroffenenrechten**
  - Verletzung von Rechten betroffener Personen
  - Verletzung von Bestimmungen zum internationalen Datenverkehr
  - Verstoß gegen die Grundsätze der rechtmäßigen Datenverarbeitung
- **Bis zu 10 Mio Euro oder 2 % des weltweiten Konzern-Jahresumsatzes**
  - **Verletzung von Pflichten des Verantwortlichen**
  - Verstoß gegen den Grundsatz „Datenschutz durch Technik und durch Voreinstellungen“
  - Verstoß gegen Bestimmungen zur Auftragsverarbeitung
  - Verletzung der Bestimmungen zum „Verzeichnis der Verarbeitungstätigkeiten“
  - Verletzung von Bestimmungen zu Datensicherheit und Datenschutz-Folgenabschätzung
- **Verschulden:** Sowohl Vorsatz als auch Fahrlässigkeit
- Geldbußen sind amtswegig durch die Datenschutzbehörden oder durch Gerichte zu verhängen
- je nachdem, welcher der Beträge höher ist.

## Datenschutzbeauftragte (Art 37 DSGVO)

- ✓ Ein/e Datenschutzbeauftragte/r ist verpflichtend zu bestellen,
  - wenn die Verarbeitung von einer **Behörde oder öffentlichen Stelle** durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,
  - wenn die **Kerntätigkeit** des Verantwortlichen/Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer **Art**, ihres **Umfangs** und/oder ihrer **Zwecke** eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
  - wenn die **Kerntätigkeit** des Verantwortlichen/Auftragsverarbeiters in der umfangreichen **Verarbeitung besonderer Kategorien von Daten** gem Art 9 und/oder Art 10 besteht
- ✓ Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten bestellen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann
- ✓ Mehrere Behörden oder öffentliche Stellen können unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe einen gemeinsamen Datenschutzbeauftragten bestellen

# Datenschutzbeauftragte Anforderungen und Stellung (Art 38 / 39 DSGVO)

## ✓ Anforderungen und Aufgaben

- Fachwissen und „Know How“ – rechtlich, technisch und kaufmännisch
- Insb. auch Datensicherheit und „Privacy by Design“
- Soll die Einhaltung der Datenschutzvorschriften durch den Verantwortlichen/Auftragsverarbeiters fördern und überwachen
- Beratung, Aufklärung und Schulung im Betrieb des Verantwortlichen
- Anlaufstelle für Aufsichtsbehörde

## ✓ Stellung

- Unabhängig und weisungsfrei (Arbeitnehmer oder externer Dienstleister)
- Darf auch andere Pflichten haben, aber keine Interessenkollisionen
- Abberufung nur wenn Voraussetzungen nach Art 37 DSGVO nicht erfüllt oder bei Entlassungsgründen
- Frühzeitige Einbindung, Zugang und Ressourcen durch Verantwortlichen zu gewährleisten
- Ansprechperson für Aufsichtsbehörden und Betroffene

## Rechtliche Anpassungen in Österreich

- ✓ **Keine „Umsetzung“ im engeren Sinn notwendig:** DSGVO ist eine EU Verordnung und bedarf keiner Umsetzung in nationales Recht → **unmittelbare Wirksamkeit**
- ✓ **Begleitgesetzgebung:** DSGVO enthält 30 explizite und viele implizite „Öffnungsklauseln“
  - Insb. „Flexibilisierungsklausel“ für den öffentlichen Sektor in Art 6 Abs. 2 DSGVO
  - Spielraum für nationale Gesetzgeber (Kritik: zu unspezifisch, keine Harmonisierung)
- ✓ **Zukünftiges nationales Datenschutzrecht in Österreich:** ein Begutachtungsentwurf der Bundesregierung wurde Mitte Mai veröffentlicht und Anfang Juni als Regierungsvorlage in den parlamentarischen Prozess verabschiedet. Der Gesetzesentwurf enthält zB Regeln bezüglich
  - Zuständigkeiten der Datenschutzbehörde
  - anzuwendendes Verfahrensrecht
  - subsidiäre Verwaltungsstrafen
- ✓ **Öffnungsklauseln (fast) nur für den öffentlichen Bereich ausdrücklich geregelt:**
  - die ausdrücklichen Öffnungsklauseln klammern weitgehend private Datenanwendungen aus (zB Videoüberwachung) → aber: Interpretativ iZm Erwägungsgrund 10
  - An vielen Stellen setzt DSGVO aber einen nationalen Rechtsbestand voraus

## Datenschutzgrundsätze (1/2)

- ✓ **Verhältnismäßigkeitsgrundsatz:** Kommt aus dem Datenschutz-Grundrecht (Art 8 Grundrechte-Charta bzw. Art 8 EMRK) und bezeichnet ein übergeordnetes Prinzip. Unter der „Verhältnismäßigkeit im engeren Sinn“ versteht man die Abwägung der Interessen bzw. Güter
- ✓ **Verbotsprinzip:** Die Verwendung personenbezogener Daten ist verboten, sofern sie nicht ausdrücklich erlaubt ist.
- ✓ **Zweckbindungsgrundsatz:** Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden.
- ✓ **Wesentlichkeitsgrundsatz:** Daten dürfen nur verwendet werden, soweit sie den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen.
- ✓ **Grundsatz der Datenlöschung:** Daten dürfen nur so lange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist.
- ✓ **Grundsatz der Datenminimierung:** Reduktion der Verarbeitung personenbezogener Daten auf das Unvermeidbare

## Datenschutzgrundsätze (2/2)

- ✓ **Privacy by Design und Privacy by Default (neu)**
- ✓ **Grundsatz von Treu und Glauben und Rechtmäßigkeit**
- ✓ **Grundsatz der Transparenz:** Information des Betroffenen über Vorhandensein einer Verarbeitung und deren Umstände
- ✓ **Grundsatz des Mitspracherechts:** Rechte auf Auskunft, Richtigstellung und Löschung sowie Widerspruch
- ✓ **Grundsatz der sachlichen Richtigkeit und Aktualität:** Daten dürfen nur so verwendet werden, dass sie im Hinblick auf den Verwendungszweck sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind.
- ✓ **Grundsatz der Datensicherheit**
- ✓ **Grundsatz der Rechenschaftspflicht**

- I. Datenschutz Grundlagen
- II. EU Datenschutzreform im Überblick
- III. DSGVO Compliance als Organisationsprojekt**
- IV. Datenschutz nach DSGVO

Quelle: Ing. Mag. Dr. iur. Christof Tschohl

## Die DSGVO in der Praxis

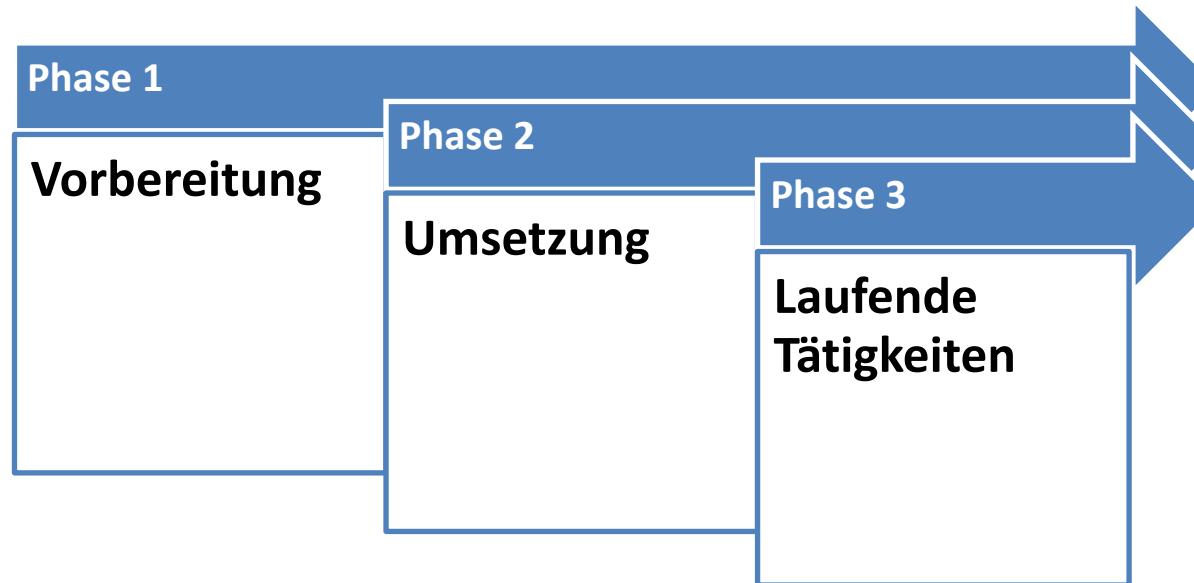
- ✓ **Vorbereitung auf die DSGVO als Organisationsprojekt**
  - Professioneller Umgang mit den Daten im Unternehmen
  - Überblick über die IT-Landschaft
  - Daten als „Asset“ des Unternehmens werden systematisch gemanagt, professionell geschützt und strategisch genutzt
- ✓ **Datenschutz-Folgenabschätzung**
- ✓ **Zertifizierung**
- ✓ **Datenschutz-Management-Software**

## 3 Phasen System

- ✓ Phase 1: Vorbereitung
- ✓ Phase 2: Umsetzung
- ✓ Phase 3: Laufende Tätigkeiten

## Allgemeines zur Planung

- ✓ Zahlreiche «Empfehlungen» und guidelines veröffentlicht
  - ✓ zB Leitlinien der französischen Aufsichtsbehörde.
  - ✓ Leitfaden des Vereines österreichischer Datenschutzbeauftragter (privacyofficers.at).
- > **3-Phasensystem:**



# Phase 1 – Vorbereitung

## ✓ Phase 1 besteht aus (zumindest) fünf Etappen

- 1.1 Management: Awareness bilden und Commitment einholen.
- 1.2 Projektauftrag für Umsetzungsprojekt einholen.
- 1.3 Benötigte Ressourcen bereitstellen.
- 1.4 Schlüsselpersonal initial schulen.
- 1.5 Prüfen, ob Datenschutzbeauftragter (DSB) notwendig ist.

## Phase 2 – Umsetzung

**Phase 2 sieht (zumindest) 15 Teilprozesse vor.**

- 2.1 Verarbeitungstätigkeiten identifizieren.
- 2.2 Verfahrensverzeichnis erstellen.
- 2.3 Risikoanalyse durchführen.
- 2.4 Einhaltung der Datenschutz-Grundsätze.
- 2.5 Datensicherheitsmassnahmen (TOM) umsetzen.
- 2.6 Betroffenenrechte wahren.
- 2.7 Einwilligungsprozess einführen.
- 2.8 Informationspflichten einführen.

## Phase 2 – Umsetzung

**Phase 2 sieht (zumindest) 15 Teilprozesse vor.**

- 2.9 Auftragsverarbeiter: Rahmenbedingungen sicherstellen.
- 2.10 Privacy by Design / Privacy by Default sicherstellen.
- 2.11 Data Breach-Prozess einführen.
- 2.12 Aufgaben des Datenschutzbeauftragten abklären.
- 2.13 Datenschutz-Policy erstellen.
- 2.14 Mitarbeiter schulen.
- 2.15 Datenübermittlung prüfen (EWR/International).

## Phase 3 – Laufende Tätigkeiten

**(Zumindest) vier relevante Ebenen.**

- 3.1 Verfahrensverzeichnis aktualisieren.
- 3.2 Audits durchführen.
- 3.3 Kontakt mit Behörden und betroffenen Personen pflegen.
- 3.4 Monitoring/Verbesserung des Datenschutz-Managementsystems.

- I. Datenschutz Grundlagen
- II. EU Datenschutzreform im Überblick
- III. DSGVO Compliance als Organisationsprojekt
- IV. Datenschutz nach DSGVO

Quelle: Ing. Mag. Dr. iur. Christof Tschohl

## Neuerungen der DSGVO im Detail

- ✓ Dokumentationspflichten:
  - Führen eines Verzeichnisses der Verarbeitungstätigkeiten (trifft nicht jedes Unternehmen, ist aber generell ratsam)
  - Dokumentation der getroffenen Maßnahmen (Datensicherheit, Privacy by Design etc.)
- ✓ Rechenschaftspflicht:
  - DSGVO-konformer Zustand muss jederzeit belegbar sein
  - Nicht nur „Data Breach“ führt zu Sanktionen
- ✓ Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten:
  - Meldung an die Aufsichtsbehörde unverzüglich, möglichst binnen 72 Stunden nachdem die Verletzung bekannt wurde
  - Benachrichtigung der Betroffenen, wenn voraussichtlich ein hohes Risiko für diese besteht
  - Impliziert auch Maßnahmen um Data Breaches überhaupt festzustellen

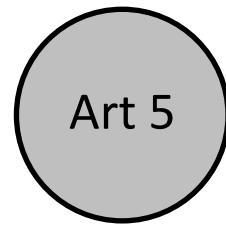
## Neuerungen der DSGVO im Detail

- ✓ Privacy by Design, d.h.:
  1. Datenschutz bei der Gestaltung von Systemen von Beginn an berücksichtigen
  2. Verhindern der nicht zweckkonformen Verwendung des Systems durch technische und organisatorische Maßnahmen
- ✓ Datenschutz-Folgenabschätzung wenn voraussichtlich ein hohes Risiko für die Betroffenen besteht:
  - Systematische Beschreibung der Verarbeitungsvorgänge
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit
  - Bewertung der Risiken für die Betroffenen
  - Abhilfemaßnahmen
- ✓ Konsultation der Datenschutzbehörde -> schriftliche Empfehlungen

# Pflichten des Verantwortlichen: Überblick und Zusammenhänge

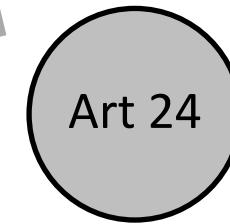
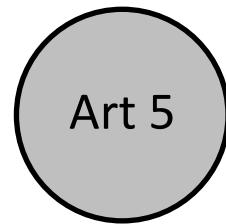
## Datenschutzgrundsätze

Eigenverantwortung des  
Verantwortlichen  
Rechenschaftspflicht



# Pflichten des Verantwortlichen: Überblick und Zusammenhänge

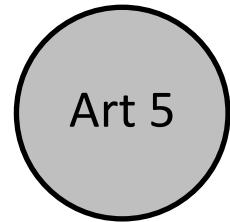
Datenschutzgrundsätze  
Eigenverantwortung des  
Verantwortlichen  
Rechenschaftspflicht



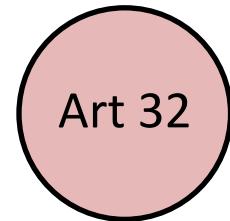
- Eigenverantwortung und Haftung des Verantwortlichen
- Technische und organisatorische Maßnahmen (TOM)
- Risikobasierter Ansatz
- Maßnahmen laufend überprüfen und aktualisieren
- Verhältnismäßigkeit

# Pflichten des Verantwortlichen: Überblick und Zusammenhänge

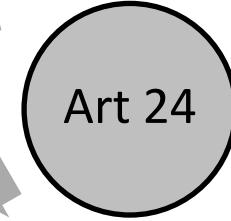
Datenschutzgrundsätze  
Eigenverantwortung des  
Verantwortlichen  
Rechenschaftspflicht



- Eigenverantwortung und Haftung des Verantwortlichen
- Technische und organisatorische Maßnahmen (TOM)
- Risikobasierter Ansatz
- Maßnahmen laufend überprüfen und aktualisieren
- Verhältnismäßigkeit

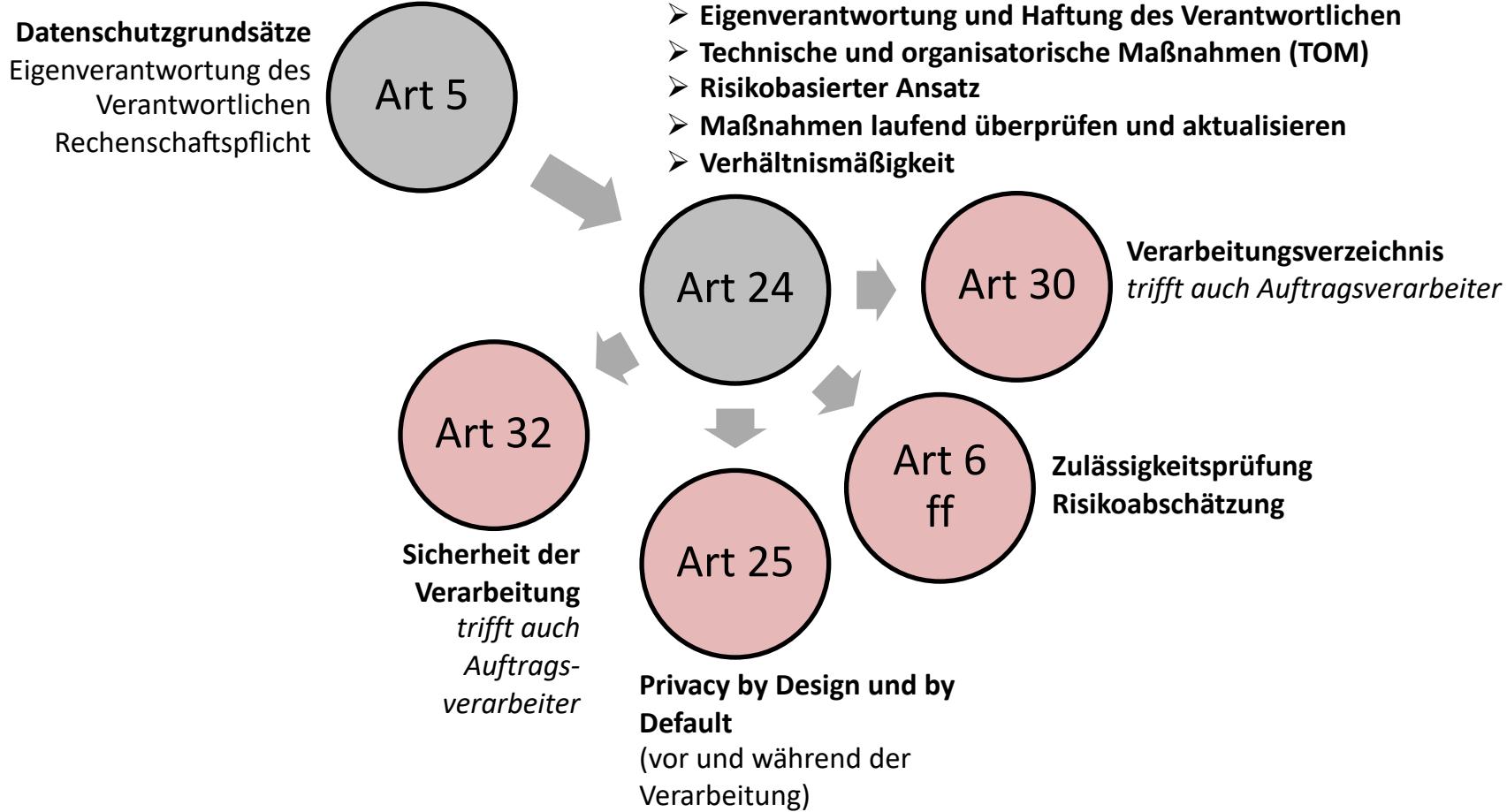


Sicherheit der  
Verarbeitung  
*trifft auch*  
Auftrags-  
verarbeiter



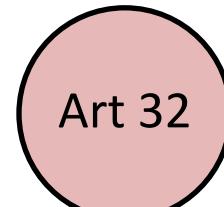
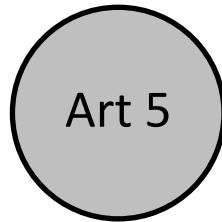
**Privacy by Design und by  
Default**  
(vor und während der  
Verarbeitung)

# Pflichten des Verantwortlichen: Überblick und Zusammenhänge

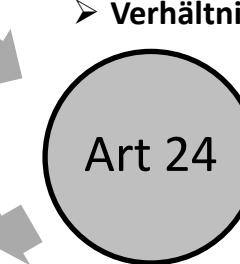


# Pflichten des Verantwortlichen: Überblick und Zusammenhänge

Datenschutzgrundsätze  
Eigenverantwortung des  
Verantwortlichen  
Rechenschaftspflicht



Sicherheit der  
Verarbeitung  
*trifft auch  
Auftrags-  
verarbeiter*



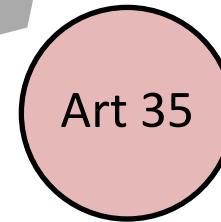
Privacy by Design und by  
Default  
(vor und während der  
Verarbeitung)

- Eigenverantwortung und Haftung des Verantwortlichen
- Technische und organisatorische Maßnahmen (TOM)
- Risikobasierter Ansatz
- Maßnahmen laufend überprüfen und aktualisieren
- Verhältnismäßigkeit



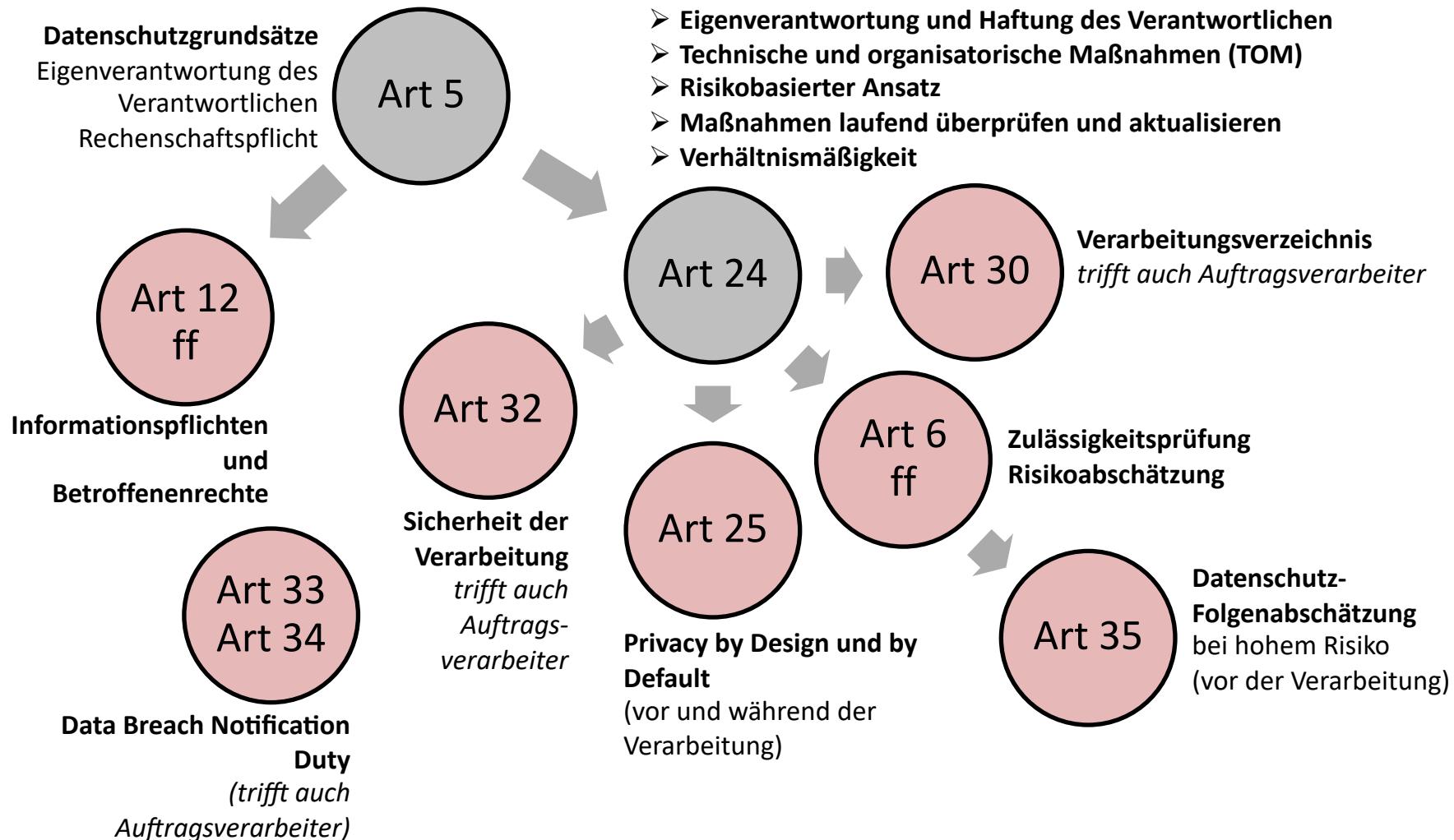
Verarbeitungsverzeichnis  
*trifft auch Auftragsverarbeiter*

Zulässigkeitsprüfung  
Risikoabschätzung



Datenschutz-  
Folgenabschätzung  
bei hohem Risiko  
(vor der Verarbeitung)

# Pflichten des Verantwortlichen: Überblick und Zusammenhänge



## Datenschutzmanagement

- Die Einhaltung dieser umfangreichen Anforderungen der DSGVO erfordert ein **systematisches, risikobasiertes Datenschutzmanagement**
- Das **Datenschutzmanagement** sollte in ähnlicher Weise umgesetzt werden, wie **andere Managementprozesse** in der jeweiligen Organisation gestaltet sind, und es sollte an diese möglichst eng anknüpfen

## Betroffenenrechte

- ✓ Recht auf Auskunft
- ✓ Recht auf Berichtigung
- ✓ Recht auf Löschung („Recht auf Vergessenwerden“)
- ✓ Recht auf Einschränkung der Verarbeitung
- ✓ Recht auf Datenübertragbarkeit
- ✓ Widerspruchsrecht

## Informationspflichten (Art 12 - 14)

- ✓ Stark ausgeweitete, aktive Informationspflicht des Verantwortlichen gegenüber der jeweils betroffenen Person (= Kunde, Bewerber, Mitarbeiter etc.)
- ✓ Ziel: transparente Datenverarbeitung (s. Art 5 Abs 1 lit a) → Betroffener soll näheren Umstände der Datenverwendung nachvollziehen können
- ✓ „How-to“ in Art 12 Abs 1: in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache, insb. an Kinder. Übermittlung erfolgt **schriftlich** oder in anderer Form, gegebenenfalls auch **elektronisch**. Falls von der betroffenen Person verlangt, kann die Information **mündlich** erteilt werden.
- ✓ Beachte: DSGVO kennt Informationspflicht bei **Direkterhebung (Art 13)** und Informationspflicht, wenn die personenbezogenen Daten **nicht (direkt)** bei der betroffenen Person erhoben werden (**Art 14**)
- ✓ Information ist grds. **unentgeltlich** zur Verfügung zu stellen (Art 12 Abs 5)

## Informationspflichten (Art 12 - 14)

Art 13 und 14 sehen **zwei „Kategorien“** von Informationen vor, über welche der Betroffenen in Kenntnis zu setzen ist:

- „**Mindestangaben**“ gem. Art 13 Abs 1 bzw Art 14 Abs 1 sind **jedenfalls** zu erteilen und
- **zusätzliche Angaben** gem. Art 13 Abs 2 bzw Art 14 Abs 2

In der Literatur herrscht Meinung vor, dass aufgrund der Tatsache, dass im Abs 2 allgemeine Hinweise zur Rechtslage gefordert werden (sowie generell aus Haftungsgründen), in der Praxis **immer** auch über diese Zusatzangaben zu informieren ist. Bis zum Erscheinen von einschlägigen Richtlinien ist die Information über **sämtliche** Angaben zu empfehlen.

Die Informationen, die den betroffenen Personen gemäß den Artikeln 13 und 14 bereitzustellen sind, können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden

Informationsinhalte von Art 13 und 14 unterscheiden sich geringfügig, im Folgenden wird nur auf Art 13 eingegangen; aber Achtung: **Informationszeitpunkt!**

## Informationspflicht bei Direkterhebung (Art 13)

### Mindestangaben zum Zeitpunkt der Erhebung zu erteilen:

- Name u. **Kontaktdaten** des Verantwortlichen sowie ggf. seines Vertreters
- **Kontaktdaten** des Datenschutzbeauftragten
- **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die **Rechtsgrundlage** für die Verarbeitung
- **berechtigte Interessen**, die von dem Verantwortlichen oder einem Dritten verfolgt werden (bei Verarbeitung gem Art 6 Ab 1 lit f)
- **Empfänger oder Kategorien von Empfängern** der Daten (bei Datenübermittlung)
- beabsichtigte Datenübermittlung in ein **Drittland** /an eine **internat. Organisation** samt **Rechtsgrundlage** hierfür (s. Art 44 ff)

### Zusätzliche Angaben zum Zeitpunkt der Erhebung zu erteilen:

- **Speicherdauer**; falls nicht möglich, Kriterien für die Festlegung dieser Dauer
- Bestehen von **Betroffenenrechten**
- Hinweis auf **Widerruf**, wenn die Verarbeitung auf Einwilligung basiert
- Bestehen eines **Beschwerderechts** bei einer Aufsichtsbehörde
- **Gesetzl. oder vertragl. Verpflichtung** zur Bereitstellung der Daten, ihrer Erforderlichkeit, Folgen der Weigerung d. Datenbereitstellung
- Bestehen einer **automatisierten Einzelfallentscheidung** gem. Art 22 Abs 1 u. 4 und über die involvierte Logik sowie die Tragweite
- [bei beabsichtigter **Weiterverarbeitung für andere Zwecke**: Informationen über anderen Zweck und alle anderen Informationen gem. Abs 2 → **vor** der Weiterverarbeitung zu informieren]

## Informationspflichten (Art 12 - 14)

- ✓ **In der Praxis:** Die Art und Form der Information ist abhängig von den konkreten Umständen, z.B. werden auf einer Website mit Newsletter-Anmeldemöglichkeit in der entsprechenden Datenschutzerklärung (welche in den Newsletter-Anmeldeprozess eingebunden wird) die o.a. Angaben aufzunehmen sein
- ✓ **Analyse** bei welchen Vorgängen personenbezogene Daten direkt von Betroffenen (Kunden, Mitarbeitern, Klienten, Patienten etc.) erhoben werden
- ✓ Je nach Medium und Kontext: passende **Datenschutzerklärung**, Datenschutz-Folder, Betriebsvereinbarung etc. zu erstellen, worin die Betroffenen informiert werden
- ✓ Entsprechende interne **Prozesse**, Schulungen etc. müssen sicherstellen, dass den Mitarbeitern das Thema „Datenschutz und Informationspflichten“ bewusst ist und die Informationspflicht auch tatsächlich eingehalten wird
- ✓ **Bei Verstoß:** Verhängung einer Geldbuße gem. Art 83 Abs 5; ev. UWG-Klage eines Konkurrenten; Verbandsklage nach dem KSchG etc.

## Recht auf Auskunft (Art 15 DSGVO)

- ✓ **Der Auskunftsgeber hat nach Art 15 DSGVO ein Recht auf Auskunft über**
  - die Verarbeitungszwecke
  - welche Daten über ihn verarbeitet werden,
  - die Quelle der Daten
  - Die Empfänger oder Kategorien von Empfängern (bei Übermittlung)
  - falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder Kriterien für deren Festlegung
  - das Bestehen von Rechten (Berichtigung oder Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht sowie Beschwerderechte)

Nach § 26 DSG zusätzlich

- auf welcher Rechtsgrundlage die Verwendung beruht,
- falls verlangt: wer als Auftragsverarbeiter herangezogen wird.

## Recht auf Berichtigung, Löschung und Einschränkung (Art 16 - 18 DSGVO)

- ✓ Unrichtige oder unzulässig verarbeitete Daten sind vom Verantwortlichen richtig zu stellen oder zu löschen
  - ✓ aus Eigeninitiative, sobald ihm die Unrichtigkeit oder die Unzulässigkeit bekannt wird, oder
  - ✓ auf begründeten Antrag des Betroffenen
    - Bei unvollständigen Daten kann das Recht auf Vervollständigung auch mittels einer ergänzenden Erklärung geltend gemacht werden
    - **Art 16 DSGVO: „Recht auf Berichtigung“**
    - **Art 17 DSGVO: „Recht auf Löschung“**
    - **Art 18 DSGVO: Recht auf Einschränkung der Verarbeitung**

## Recht auf “Vergessenwerden” (Art 17 DSGVO)

### ✓ „Recht auf Vergessenwerden“

- Lange im Reformprozess diskutiert, dann ein Vorstoß des EuGH
- Normiert in Art 17 Abs. 2 DSGVO: Verantwortlicher muss sich auch mit (zumutbaren) technischen Mitteln dafür einsetzen, dass die Veröffentlichung Rückgängig gemacht wird
- Abwägung mit Informationsfreiheit (Art 17 Abs. 3 DSGVO)

- ### ✓ Urteil des **EuGH** (Große Kammer) vom 13. Mai 2014 in der Rechtssache C-131/12, **Google Spain SL** und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González
- Bemerkenswert: Google unterliegt der EU Jurisdiktion und dem Datenschutzrecht, auch wenn in der EU nur eine Vertriebsniederlassung liegt
  - Trefferliste zur Personensuche ist eine neue Informationskategorie und lässt das “Schutzwürdige Geheimhaltungsinteresse” (vgl. § 1 DSG) “wieder auflieben”
  - Bedeutung für Ausnahme “öffentliche verfügbarer Daten” aus dem Schutzbereich?

## Verzeichnis von Verarbeitungstätigkeiten (Art 30)

### ✓ Bis 24.5.2018: Datenverarbeitungsregister (DVR)

- ✓ Pflicht zur Meldung von Datenanwendungen im öffentl. zugängl. DVR gemäß §§ 17 ff DSG 2000 → Exportfunktion aus DVR-Online bis 31.12.2019

### ✓ Ab 25.5.2018: internes Verarbeitungsverzeichnis („VVZ“):

- ✓ Zu führen und zu aktualisieren vom **Verantwortlichen** und (neu!) **Auftragsverarbeiter**, aber mit unterschiedlichem Dokumentationsumfang (Art 30 Abs 1 vs. Abs 2)
  - ✓ **Schriftlich** zu führen, auch elektronische Führung zulässig; nicht-öffentliche
  - ✓ Ist Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen (Art 30 Abs 4)
  - ✓ **Ausnahme** von Dokumentationspflicht → gilt **nicht** für Unternehmen, die weniger als **250** Mitarbeiter beschäftigen, **es sei denn (Rückausnahmen!):**
    - die von ihnen vorgenommene Verarbeitung birgt ein **Risiko für die Rechte und Freiheiten** der betroffenen Personen;
    - die Verarbeitung erfolgt **nicht nur gelegentlich** oder
    - es erfolgt eine Verarbeitung **besonderer Datenkategorien** gemäß Art 9 Abs 1 bzw. die Verarbeitung von personenbezogenen **Daten über strafrechtliche Verurteilungen und Straftaten** iSd Art 10
- **Achtung! Betroffenenrechte (Auskunftsrecht etc) bestehen weiterhin, Dokumentation erforderlich**

## Verzeichnis von Verarbeitungstätigkeiten (Art 30)

### Mindestinhalt des VVZ des Verantwortlichen (Art 30 Abs 2):

- den **Namen u. die Kontaktdaten des Verantwortlichen** u. ggf. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen **Datenschutzbeauftragten**;
- die **Zwecke** der Verarbeitung;
- eine **Beschreibung der Kategorien betroffener Personen** u. der **Kategorien pers.bez. Daten**;
- die **Kategorien von Empfängern**, gegenüber denen die pers.bez. Daten offengelegt worden sind oder noch offengelegt werden, einschließlich **Empfänger in Drittländern/internat. Organis.**
- ggf. **Übermittlungen von personenbezogenen Daten an ein Drittland** oder an eine internat. Organis., einschließlich der Angabe des Drittlands oder der internat. Organis. (+ Dokumentierung geeigneter Garantien bei Übermittlungen gem Art 49 Abs 1 UAbs 2);
- wenn möglich, die vorgesehenen **Fristen für die Löschung** der verschiedenen Datenkategorien;
- wenn möglich, eine **allgemeine Beschreibung der technischen und organisatorischen Maßnahmen** gemäß Art 32 Abs 1

**Empfehlenswert** ist Erweiterung um zusätzliche Angaben der Art 13 ff DSGVO, wie z.B. Rechtsgrundlage der Verarbeitung, Herkunft der Daten

## Verzeichnis von Verarbeitungstätigkeiten (Art 30)

### ✓ Mindestinhalt des VVZ des Auftragsverarbeiters (Art 30 Abs 3):

- **Namen und die Kontaktdaten des Auftragsverarbeiters** oder der Auftragsverarbeiter und jedes **Verantwortlichen**, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
- die **Kategorien von Verarbeitungen**, die im Auftrag jedes Verantwortlichen durchgeführt werden;
- gegebenenfalls **Übermittlungen** von personenbezogenen Daten an ein **Drittland** oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation (+ Dokumentierung geeigneter Garantien bei Übermittlungen gem Art 49 Abs 1 UAbs 2);
- wenn möglich, eine **allgemeine Beschreibung der technischen und organisatorischen Maßnahmen** gemäß Art 32 Abs 1

## Verzeichnis von Verarbeitungstätigkeiten (Art 30)

- ✓ **VVZ ist Grundstein der DSGVO-Compliance u.a. in Hinblick auf:**
  - ✓ Einhaltung Nachweis- u. Rechenschaftspflicht (Art 5 Abs 2)
  - ✓ (fristgerechte) Erfüllung der Betroffenenrechte (Art 12 ff)
  - ✓ Datenschutz-Folgenabschätzung (Art 35 f)
- ✓ **Verfahrensverzeichnis besteht mindestens aus 3 aufeinander aufbauenden Teilen [nach Schäffter 2016]:**
  - Allgemeiner, verfahrensübergreifender Teil
  - Spezifische Angaben zu den einzelnen Verfahren/Verarb.tätigkeiten
  - Angaben zu techn. u. organisator. Maßnahmen (TOM)

## Sachlicher Anwendungsbereich DSGVO I

- ✓ Ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten
- ✓ Nichtautomatisierte Verarbeitung personenbezogener Daten,
  - Wenn die Verarbeitung in einer Daten gespeichert sind, oder gespeichert werden sollen (Art 2 Abs 1 DSGVO) – „manuell strukturierte“ Daten
  - das bedeutet: **unstrukturierte Verarbeitung personenbezogener Daten unterliegt immer dem Grundrecht auf Datenschutz aber nicht der DSGVO (bzw. nicht dem einfachgesetzlichen Teil des DSG 2000)**
- ✓ Art 4 Abs 1 DSGVO:
  - „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen;
  - als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, [...] identifiziert werden kann

## Sachlicher Anwendungsbereich DSGVO II

- ✓ Verarbeitung personenbezogener Daten unabhängig von Staatsangehörigkeit oder Aufenthaltsort
- ✓ Kein Schutz juristischer Personen (sehr wahrscheinlich auch nicht mehr in Österreich)
- ✓ Im Ergebnis ein sehr weiter Verarbeitungsbegriff
- ✓ Speicherung als Datei umfasst sowohl automatisierte – als auch manuelle Verarbeitung
- ✓ Art 4 Abs 6 DSGVO:
  - „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

## Ausnahmen vom sachlichen Anwendungsbereich

- ✓ Art 2 Abs 2 DSGVO:
  - Tätigkeiten außerhalb des Unionsrechts (lit a)
    - ✓ Nationale Sicherheit
  - Tätigkeiten im Anwendungsbereich von Titel V Kapitel 2 EUV (lit b)
    - ✓ gemeinsames Außen- und Sicherheitspolitik
  - Tätigkeiten von natürlichen Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (lit c)
    - ✓ soziale Netzwerke
  - Tätigkeiten von Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten (lit d)

## Räumlicher Anwendungsbereich DSGVO I

- ✓ [...] im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet (Art 3 Abs 1 DSGVO)
- ✓ Rechtsform unerheblich
- ✓ Auch Zweigstelle oder Tochtergesellschaft umfasst
- ✓ Niederlassung außerhalb der EU
  - Ebenfalls anwendbar, wenn die Datenverarbeitung dazu dient,
    - ✓ betroffenen Personen in der Union **Waren oder Dienstleistungen anzubieten**, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist (lit a)
    - ✓ das Verhalten **betroffener Personen zu beobachten**, soweit ihr Verhalten in der Union erfolgt (lit b)

## Räumlicher Anwendungsbereich DSGVO II

Anwendungsbereich DSGVO im Überblick:

- Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung in der EU
- Wenn keine Niederlassung in der EU: Anbieten von Waren oder Dienstleistungen in der EU
- Beobachten des Verhaltens von Betroffenen in der EU

Angebot von Waren oder Dienstleistungen (lit a) (Indizien)

- Verwendung von Sprache, Verwendung von Währungen, Möglichkeit der Bestellung in dieser Sprache/Währung

Beobachtung von Verhalten (lit b) (Indizien)

- Nachvollziehbarkeit der Internetaktivität
- Profilerstellung durch verwendete Datenverarbeitungstechniken zur Bildung einer Entscheidungsgrundlage, Analyse der Vorlieben oder Verhaltensweisen

## Art 4 Z 2 DSGVO – (Daten)Verarbeitung

- ✓ „**Verarbeitung**“: jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung; (vergleiche § 4 Z 7 DSG: Definition „Datenanwendung“)
- ✓ **Beispiele:**
  - Personalverwaltung, Kundendatenbanken, Organisationsprogramme (SAP, Navision, Advokat, etc.), Zeiterfassungssysteme, Patientenverwaltung, Mitgliederverwaltung, Videoüberwachung, Kennzeichenerfassung, uva
  - Komplexität und Interdependenz von Datenanwendung: Cloud Computing, verteilte Systeme, Datawarehouse, Datamining, „Big Data“,...

## Datenarten – Definitionen gem Art 4 DSGVO

- ✓ Art 4 Abs 1 DSGVO: „**Personenbezogene Daten**“ sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“
  - identifiziert = der Person unmittelbar zugeordnet
  - identifizierbar = natürliche Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann
- ✓ Bisheriges Konzept „Indirekt personenbezogene Daten“ nach dem DSG 2000: Personenbezog kann mit rechtlich zulässigen Mitteln nicht hergestellt werden (pseudonymisierte Daten)
  - Nach DSG bisher erhebliche Erleichterung: keine schutzwürdigen Geheimhaltungsinteressen; keine Auskunft, Richtigstellung und Löschung, generell zulässig für Forschung
- ✓ anonymisierte Daten: Identität für Niemanden erschließbar – nicht im Schutzbereich

## Pseudonymisierung und Anonymisierung

- ✓ Definition „Pseudonymisierung“ Art 4 Z 5 DSGVO:
  - Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung von Zusatzinformationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können“ (und gesonderte Aufbewahrung dieser Zusatzinformationen), reduziert jedenfalls das Risiko
- ✓ Anonymisierung: Zuordnung zur betroffenen Person mit Mitteln, die nach allgemeinem Ermessen wahrscheinlich genutzt werden könnten, nicht möglich (Datenschutzrecht nicht mehr anwendbar)
- ✓ Trend: Datafication
  - Immer mehr personenbezogene Daten werden erhoben
  - und sind in vielen Fällen im Internet auffindbar – Menge der Zusatzinformationen ist enorm
- ➔ Anonymisierung und Pseudonymisierung müssen richtig gemacht werden um wirksam zu sein und dürfen nicht als bloßes Feigenblatt dienen
- ➔ Anonymisierung oft unmöglich, wenn eine gewisse Aussagekraft erhalten werden soll
- ➔ Aggregation der Daten als Alternative (sofern tunlich)

## Pseudonymisierung nach DSGVO im Verhältnis zu „indirekt personenbezogenen Daten“ nach DSG

### Pseudonymisierung: Von der Option der Privilegierung (DSG: indirekt personenbezogene Daten) zur verpflichtenden Sicherheitsmaßnahme

- ✓ Personenbezogene Daten sind zu pseudonymisieren, wenn der konkrete Verarbeitungszweck auch mit pseudonymisierten Daten zu erreichen ist (sofern kein unverhältnismäßig hoher Aufwand)
- ✓ Art 4 Z 5:  
„Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten **ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können**, sofern diese **zusätzlichen Informationen gesondert aufbewahrt** werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“
- ✓ Pseudonymisierung ist schwierig: Auch wenn identifizierende Attribute (Name etc.) entfernt werden, kann aus den Daten selbst heraus eine Zuordnung zum Betroffenen möglich sein (zB individuelle medizinische Daten)

## Besonders schutzwürdige Daten nach der DSGVO

- ✓ Art 9 DSGVO „Verarbeitung besonderer Kategorien personenbezogener Daten“ (bisher nach DSG „sensible Daten“)
  - rassische/ethnische Herkunft, politische Meinung, religiöse/weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, genetischen/biometrischen Daten, Gesundheitsdaten, Daten zum Sexualleben/sexuelle Orientierung
  - **Grundsätzlich UNTERSAGT, aber:**
  - Ausnahmen in Abs 2, zB Einwilligung (grundsätzlich strenger als DSG)
  - Abs 4 gibt den Mitgliedstaaten das Recht, weitere Bedingungen/Beschränkungen einzuführen/aufrechtzuerhalten

## Datenarten – „sensible Daten“ nach DSG

- ✓ „**Sensible Daten**“ („besonders schutzwürdige Daten“): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;
- ✓ **Erhöhter Schutz nach dem DSG 2000**
  - Vorabkontrolle durch Datenschutzbehörde (DSB) gem. § 18 (2) DSG
  - Jederzeitige Kontrollbefugnis der DSB gem. § 30 DSG
  - Strengere Voraussetzung zur Zulässigkeit der DV bzw. –Verwendung (§ 9 DSG)
- ✓ **Strafrechtsbezogene Daten** (§ 18 (4) DSG)
  - Ähnlich den sensiblen Daten (nicht in der DS-Richtlinie, Kompetenzgründe)
  - Ebenfalls Vorabkontrolle durch die DSB (§ 18 (2) Z 2 DSG)

## Rollen im Datenschutzrecht

Definitionen gemäß Art 4 DSGVO, Konkretisierung durch Judikatur

**„Betroffene Person“:** jede vom Verantwortlichen verschiedene natürliche Person, deren Daten verarbeitet werden

**„Verantwortlicher“**

die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

Wer entscheidet, welche Daten für welche Zwecke wie verarbeitet werden?

„Entscheidung“ weit zu verstehen: auch bei gesetzlichen Pflichten (dann kann aber auch das Gesetz festlegen, wem die Rolle des Verantwortlichen zukommt)

Natürliche Personen, juristische Personen und Personengemeinschaften (ARGE), Organe einer Gebietskörperschaft und deren „Hilfsapparate“ (zB Krankenanstalt)

**„Auftragsverarbeiter“:** eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet; (zB auch Hosting, Cloud-Dienste, etc)

# Auftragsverarbeitung

## ✓ Derzeitige Regelung im DSG 2000:

- „**Auftraggeber**“ (§ 4 Z 4): „Herr der Daten“; „**Dienstleister**“ (§ 4 Z 5)
- „**Überlassen** von Daten“ (§ 4 Z 11): die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses (≠ Übermittlung)
  - Auftraggeber überlässt Dienstleister personenbezogene Daten nur zur Herstellung eines dem Dienstleister aufgetragenen Werkes; Sonderfall „Ermittlungsdienstleister“
- §§ 10 f: Auswahl und Pflichten des Dienstleisters
- **Im Ergebnis:** „Privilegierung“, da keine gesonderte Rechtsgrundlage für Überlassung an Dienstleister (und auftragsgemäße Verarbeitung) erforderlich

## ✓ Datenschutz-Grundverordnung - Auftragsverarbeitung

- Geregelt in **Art 28, 29 DSGVO** (Achtung: relevante Bestimmungen finden sich z.B. auch in Art 32, 33, 37, 38, 60 Abs 10; § 6 Abs 2 DSG neu: Datengeheimnis)
- „**Verantwortlicher**“ (Art 4 Z 7): entscheidet allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten
- „**Auftragsverarbeiter**“ (Art 4 Z 8): verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen
- **Unverändert:** Verarbeitung nur auf Weisung des Verantwortlichen
- **Privilegierung** bleibt bestehen (*Albrecht/Jotzo*), auch wenn der DSGVO der Begriff der Überlassung unbekannt ist (Auftragsverarbeiter ist nicht „Dritter“ iSv Art 4 Z 10)

## Auftragsverarbeitung: Anforderungen der DSGVO

- ✓ **Sorgfältige Auswahl des Auftragsverarbeiters durch Verantwortlichen (Art 28 Abs 1; vgl bereits § 10 Abs 1 DSG 2000):**
  - Gestiegene Bedeutung durch DSGVO (Anforderungen an Vertrag, Sanktionsregime etc)
  - Hinreichende Garantien dafür, dass **geeignete technische und organisatorische Maßnahmen** (TOM) so durchgeführt werden, dass die Verarbeitung durch Auftragsverarbeiter im Einklang mit den Anforderungen dieser Verordnung erfolgt und **Schutz der Betroffenenrechte** gewährleistet ist → möglicher Nachweis durch: Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42
- ✓ **Schriftlicher Vertrag** zwischen Verantwortlichem und Auftragsverarbeiter (Art 28 Abs 3 und 9) oder „ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten“
  - Auch in elektron. Format möglich (Art 28 Abs 9, z.B. unterschriebenes PDF per E-Mail)
  - Zwingende Mindestinhalte (siehe nächste Folie)
  - Empfehlung: Nicht nur Mindestinhalte gem Art 28 Abs 3 zu beachten (Art 27, 32, 33, 37 etc)
- ✓ **Auftragsverarbeiter im Drittland:** Regelungen für grenzüberschreitenden Datenverkehr beachten (Art 44 ff); tlw. Entfall der Genehmigungspflicht durch DSB

## Mindestinhalte des Auftragsverarbeitungsvertrags (Art 28 Abs 3)

- ✓ Gegenstand und Dauer der Verarbeitung
- ✓ Art und Zweck der Verarbeitung
- ✓ Art der personenbezogenen Daten
- ✓ Kategorien betroffener Personen
- ✓ Pflichten und Rechte des Verantwortlichen
- ✓ Verarbeitung nur auf dokumentierte Weisung(en) des Verantwortlichen (lit a)
- ✓ Verpflichtung der Mitarbeiter des Auftragsverarbeiters zur Vertraulichkeit (lit b)
- ✓ Einhaltung erforderlicher Maßnahmen gem Art 32 (Datensicherheit; lit c)
- ✓ Einhaltung der Vorgaben gem Art 28 Abs 2 u 4 bei Sub-Auftragsverarbeitern (lit d)
- ✓ Unterstützung des Verantwortlichen bei Wahrung der Betroffenenrechte (lit e)
- ✓ Unterstützung bei Sicherheit, Data Breach, Datenschutz-Folgenabschätzung (lit f)
- ✓ Datenlöschung bzw -rückgabe nach Erbringung der Verarbeitungsleistungen (lit g)
- ✓ Zurverfügungstellung aller erforderlichen Informationen und Ermöglichung von Überprüfungen bzw Inspektionen (lit h)
- ✓ **[§ 6 DSG neu:** Verpflichtung der Mitarbeiter auf Datengeheimnis; Belehrung]

## Auftragsverarbeiter: Pflichten, Haftung etc.

- ✓ Verstößt ein Auftragsverarbeiter gegen DSGVO und bestimmt selbst Zwecke und Mittel der Verarbeitung → Verantwortlicher (ex lege: Art 28 Abs 10)
- ✓ **Haftung** (Art 82): Solidarische Außenhaftung von Auftragsverarbeiter **und** Verantwortlichem → Regressanspruch im Innenverhältnis
- ✓ **Sub-Auftragsverarbeiter** („weiterer Auftragsverarbeiter“, Art 28 Abs 2):
  - Vorherige schriftliche Genehmigung des Verantwortlichen erforderlich
  - Vertrag zwischen AV und Sub-AV muss dieselben Datenschutzpflichten enthalten wie im Auftragsverarbeitungsvertrag zwischen Verantwortlichem und AV (Art 28 Abs 4); TOM müssen DSGVO-Anforderungen entsprechen
  - „Erster“ Auftragsverarbeiter haftet gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-AV (Art 28 Abs 4)
- ✓ **Selbständige Pflichten des Auftragsverarbeiters** (Auswahl)
  - NEU: Erstellung eines Verarbeitungsverzeichnisses (Art 30 Abs 2, siehe Abs 5)
  - NEU: ev. Benennung Datenschutzbeauftragter (Art 37 Abs 1)
  - Gewährleistung der Sicherheit der Verarbeitung (Art 32 Abs 1)
  - Meldung von Datenschutzverletzungen an Verantwortlichen (Art 33 Abs 2)

# Auftragsverarbeitung: Handlungsempfehlungen

- ✓ **IST-Zustand erheben:** Welche Dienstleisterverträge bestehen?
- ✓ **GAP-Analyse:** Prüfung auf Konformität mit den Anforderungen der DSGVO, besteht Anpassungsbedarf? → im Regelfall zu bejahen, wenn bislang Muster der Datenschutzbehörde öä verwendet wurde
- ✓ **Weitere wichtige Schritte strategisch planen:**
  - Eigenes Vertragsmuster erstellen (bis 25.5.2018: „doppelgleisig“ DSG 2000 und DSGVO)
  - Kontakt mit Auftragsverarbeiter(n) aufnehmen; große Auftragsverarbeiter werden ihr eigenes Muster einsetzen wollen (Achtung auf Abweichungen von den Vorgaben der DSGVO bzgl Haftung etc)
  - Dokumentation insbesondere der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters
  - Laufende Kontrolle des Auftragsverarbeiters
  - Verzeichnis der Verarbeitungstätigkeiten: Auftragsverarbeiter-Tätigkeiten berücksichtigen
  - Einbindung bei Durchführung einer Datenschutz-Folgenabschätzung
- ✓ **Sanktionsmöglichkeit auch für Verletzung von Handlungspflichten, nicht nur bei Data Breach!**
- ✓ **Mustervertrag nach DSGVO der WKO:**
  - <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag.html>

## Gemeinsam für die Verarbeitung Verantwortliche

**Artikel 26 DSGVO:** *keine echte Nachfolgeregelung zum „Informationsverbundsystem“, keine Vorabkontrollpflicht*

- ✓ (1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.
- ✓ (2) Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.
- ✓ (3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

## Informationsverbundsysteme § 4 Z 13 und § 50 DSG

„Informationsverbundsystem“: die **gemeinsame Verarbeitung** von Daten in einer Datenanwendung durch **mehrere Auftraggeber** und die **gemeinsame Benutzung** der Daten in der Art, dass **jeder Auftraggeber** auch auf jene Daten im System **Zugriff** hat, die **von den anderen Auftraggebern** dem System zur Verfügung gestellt wurden (DSGVO: kein „Informationsverbundsystem“ aber Regeln zur gemeinsamen Verarbeitung und zur Verteilung der Verantwortung)

**Beispiele** im öffentlich-rechtlichen und privaten Bereich:

Führerscheinregister, zentrale Melderegister, „Klein-Kredit Evidenz“ (KKE), „Zentrales Informationssystem des Verband der Versicherungsunternehmen Österreichs (VVO), gemeinsame Kundendatenbanken, gemeinsame Zutrittskontrollverwaltung,...

### Pflichten

- Geeigneten Betreiber bestellen (§ 50 DSG)
- Meldepflicht und Vorabkontrolle bei DSB (§ 18 (2) Z 4 DSG)

## Eingriffe in das Datenschutzgrundrecht

- ✓ *Jede Verwendung von personenbezogenen Daten im Schutzbereich (Ermittlung, Verarbeitung, Weitergabe)*
- ✓ „Zweckänderung“ einer Datenverarbeitung ist ein eigenständiger Eingriff (Widmungsänderung bedarf neuerlicher Rechtfertigung)
- ✓ Rechtsschutz durch **Datenschutzbehörde** (DSB) – oder derzeit noch nach DSG 2000 gegen private Rechtsträger durch **Zivilgerichte**

## Rechtfertigung der Datenverarbeitung

- ✓ **Eingriffe in das Grundrecht auf Geheimhaltung sind zulässig wenn**
  - der Betroffene seine Zustimmung gegeben hat,
  - lebenswichtige Interessen des Betroffenen die Verwendung seiner Daten erfordern oder
  - überwiegende berechtigte Interessen eines anderen an der Datenverwendung vorliegen.
- ✓ **Jede Verwendung personenbezogener Daten bedarf einer besonderen Rechtsgrundlage!**
- ✓ Datenverwendung durch staatl. Behörden *nur aufgrund von Gesetzen, die notwendig iSd Art 8 Abs. 2 EMRK sind (öffentliches Interesse)*

## Einwilligung (Art 4 Z 11 DSGVO)

- ✓ „**Einwilligung**“ der betroffenen Person: „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“
- ✓ **Informierte Einwilligung** (siehe nächste Folie)
- ✓ Kann fehlende Rechtsgrundlagen (Gesetze, Verordnung, Statuten, etc) grundsätzlich ersetzen
- ✓ Ausdrücklich (bei „sensiblen Daten“ immer) oder konkludent
  - Problem „opt in“ / „opt out“ – Datenschutz als „Voreinstellung“!?
- ✓ Art 4 Abs 2 iVm Art 7 DSGVO: zumindest konkludent, möglichst keine voreingestellten Häkchen (ausdrücklich nur in Erwägungsgrund 32)

## Bedingungen der Einwilligung (Art 7 DSGVO)

### ✓ Informierte Einwilligung

- Anforderungen an das Ersuchen um Einwilligung
  - ✓ in verständlicher und leicht zugänglicher Form
  - ✓ in einer klaren und einfachen Sprache
  - ✓ von den anderen Sachverhalten klar zu unterscheiden
  - ✓ Zweck der Datenanwendung und Datenarten
  - ✓ Übermittlungsempfänger und Übermittlungszwecke
- Beweislast des Verantwortlichen, die Einwilligung nachzuweisen
- Getrennte Einwilligung für verschiedene Zwecke (vgl. Art 7 Abs. 2 DSGVO und ausdrücklich in Erwägungsgrund 32)
- Keine Junktimierung: wenn die Datenverarbeitung zur Vertragserfüllung nicht erforderlich ist („Koppelungsverbot“, Art 7 Abs. 4 DSGVO)
- Hinweis auf jederzeitigen Widerruf

## Widerspruch nach der DSGVO

- ✓ Widerspruch Art 21 Abs. 1 DSGVO → bis Widerruf, rechtmäßige Verarbeitung
- ✓ Nach Widerspruch:
  - Verarbeitung nur mehr bei berechtigten Interessen des Verantwortlichen
- ✓ Voraussetzungsloses und uneingeschränktes Widerspruchsrecht bei Direktmarketing & Profiling
- ✓ Hinweis auf Widerspruchsrecht nach Art 21 Abs. 4 DSGVO
- ✓ Einschränkungen durch nat. Gesetze nach Art 23 DSGVO  
(Verhältnismäßigkeitsgrundsatz & Wesensgehalt)

## Exkurs: Direktmarketing und „cold calling“

- ✓ Verbot des „cold calling“ nach § 107 TKG (Telekommunikationsgesetz):
  - Grundsätzliches Verbot von Anrufen zu Werbezwecken ohne Einwilligung
  - Einwilligung grundsätzlich auch konkludent (Beweislast beim Anrufer)
  - Transparenz, von welchen Unternehmen Werbung zu erwarten ist und welche Produkte dabei beworben werden (OGH 19. 3. 2013, 4 Ob 13/13k)
  - Deutliche Erleichterungen für „elektronische Post“ – im Rahmen von bestehenden Beziehungen (bei sachlichem Zusammenhang)
  - Privilegierung von Direktmarketingunternehmen / Adressverlagen (§ 151 Gewerbeordnung)

## Automatisierte Entscheidungen im Einzelfall

Profiling gem Art 22 DSGVO

- Die **betroffene Person** hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden **Entscheidung unterworfen zu werden**, die ihr gegenüber **rechtliche Wirkung entfaltet** oder sie in ähnlicher Weise erheblich beeinträchtigt.

Definition in Art 4 Abs. 4 DSGVO

- Jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden,
- um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich
- Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel
- dieser natürlichen Person zu analysieren oder vorherzusagen

## Profiling Automatisierte Entscheidungen im Einzelfall

- ✓ Art. 22 DSGVO, Art. 11 DSRL-PJ, Art. 15 DSRL sowie Art. § 49 DSG
- ✓ Verbot von Entscheidungen, die
  - ausschließlich auf einer automatisierten Verarbeitung beruhen und
  - dem Betroffenen gegenüber rechtliche Wirkungen entfalten oder ihn erheblich beeinträchtigen
- ✓ Ausnahmen Art 22 Abs 2 DSGVO
  - Abschluss oder Erfüllung eines Vertrags
  - Ausdrücklich vorgesehen in Rechtsvorschriften der Union oder der Mitgliedstaaten, die angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten
  - Ausdrückliche Einwilligung der betroffenen Person

# Haftung Handlungspflichten und Gestaltungsspielräume

- ✓ Interne Richtlinien und Organisations-Policy
  - **IT Sicherheitsrichtlinie**
  - **Konkrete Sicherheitsmaßnahmen**
  - **Definition von Rollen und Sicherheitsklassen** (Administrator, Bereichsleiter, etc)
  - Sicherstellung der Compliance va durch Schulungsmaßnahmen und Information
- ✓ **Absicherung nach Innen**
  - Dokumentation (Risk Assessment, Weisungen, Prüf- und Warnpflichten, etc)
  - Zertifizierungen von Anwendungen, Produkten, Management-Systemen
  - Externe Audits und Beratung durch Fachleute
- ✓ **Absicherung nach Außen**
  - Haftungsausschlüsse und Beweislastregeln in Verträgen, AGB, EULA, etc.
  - “Outsourcing” durch Dienstleisterbestellung; Versicherungen
  - Service-Level-Agreement (SLA), Garantien, Vertragsstrafen, etc.

## Haftung und Schadenersatz (Art 82 DSGVO)

- ✓ Schadenersatz – nur dem Grunde nach in der DSGVO, ansonsten nach nationalem Recht
  - **Kausalität** (Verursachung)
  - **Rechtswidrigkeit** in Bezug auf gesetzliche oder vertragliche Bestimmungen
  - **Verschulden** (leichte/grobe Fahrlässigkeit, Vorsatz)
- ✓ Schaden
  - **Konkreter Vermögensschaden** – bei schwerem Verschulden (Vorsatz und grober Fahrlässigkeit) auch entgangener Gewinn
  - **Immaterieller Schaden**
    - ✓ Vgl. § 1328a ABGB: bei erheblicher Verletzung der Privatsphäre (insb. Bloßstellung in der Öffentlichkeit) – zB geheime Tonbandaufnahme eines vertraulichen Gesprächs
    - ✓ Vgl. § 33 DSG: Grundsätzlich Verweis auf ABGB
    - ✓ Judikatur: bei Bloßstellung in der Öffentlichkeit analog zu § 7 Mediengesetz, wenn die Veröffentlichung nicht im Anwendungsbereich des Mediengesetzes erfolgt

# Haftung organisatorisch

- ✓ Haftung im Unternehmen
  - **Unternehmensleitung** (Vorstand, Geschäftsführung)
  - **Dienstnehmerhaftung** (unabhängig von "Auswahlverschulden")
    - ✓ Haftungsrückgriff und Beschränkung nach DHG – bei entschuldbaren Fehlleistungen / milderer Grad des Versehens
- ✓ **Verbandsverantwortlichkeitsgesetz (VbVG)**
  - Entscheidungsträger
    - ✓ Vorstand, GF, Prokurist oder wer sonst maßgeblichen Einfluss auf die Geschäftsführung ausübt
    - ✓ Sanktion: Geldbuße (unabhängig von allfälligen Strafverfahren gegen DN, bei Sorglosigkeit auch Haftung für Handlungen der Mitarbeiter)
- ✓ **Verwaltungsstrafverfahren**
  - Vertretungsbefugte Organe
  - Verantwortlicher Beauftragter gem. § 9 (2) Verwaltungsstrafgesetz (VStG)
  - Nachweisliche Zustimmung und entsprechende Anordnungsbefugnis im Unternehmen

## Geldbußen (Art 83 DSGVO)

- ✓ Hohe Strafandrohungen
  - **Bis zu 20 Mio Euro oder 4 % des weltweiten Konzern-Jahresumsatzes**
    - je nachdem, welcher der Beträge höher ist.
  - **Verschulden:** Sowohl Vorsatz als auch Fahrlässigkeit
  - Geldbußen sind amtswegig durch die Datenschutzbehörden oder durch Gerichte zu verhängen

# Sicherheit für den GDA

Vorgangsweise für die Umsetzung

# Kontrollbereiche des Datenschutzes

- Recht:
  - behandeln rechtliche Anforderungen
- Organisation:
  - verschiedene Verantwortungsbereiche in der Organisation
- Prozesse:
  - wiederkehrende Kontrollen und Maßnahmen
- IKT:
  - Anforderungen an IKT-Anwendungen

# Betroffenenrechte

- Informationen sind in präziser, transparenter, verständlicher und leicht zugänglich sowie einfacher Sprache zu übermitteln ... Der Verantwortliche hat die Ausübung der Rechte der betroffenen Person zu erleichtern – Art 12.
- Informationspflicht – Art 13 und Art 14
- Auskunftspflicht – Art 15
- Recht auf **Vergessen** – Art 17
- Recht auf **Datenübertragbarkeit** – Art 20
- **Pflicht Implementierung Datenschutzrichtlinie**

# Aufbewahrung von Daten

- Sicherheit von Daten – Art 4 Z 12
  - zum Schutz gegen Verletzung der CIA-Triade unabsichtlich oder unrechtmäßig
- Speicherbegrenzung – Art 5 Abs 1e
  - die Identifizierung der betroffenen Person(en) nur so lange ermöglichen, wie es für die Verarbeitung notwendig ist

# Datenschutz Folgenabschätzung

- ist eine **neue Pflichttätigkeit** des Verantwortlichen, um bei einem **hohen Risiko** die **persönlichen Rechte und Freiheiten** einer betroffenen Person durch die Verarbeitung nicht **zu verletzen**
- die DSGVO verlangt Mindestinhalte in der Folgenabschätzung
  - systematische Beschreibung der geplanten Verarbeitungsvorgänge
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit
  - Risikobewertung und Maßnahmen zum Schutz der personenbezogenen Daten

# Datenschutzkonzept & -management

- Datenschutz muss durch ein strukturiertes System und nicht anlassbezogen erfolgen
- Diese „neue“ Datenschutzkultur erfordert eine Verknüpfung der Unternehmensbereiche
  - Recht,
  - Organisation,
  - Projekte / Prozesse und
  - IKT
- Ein Integriertes Managementsystem mind. zwischen ISMS und DSMS bzw. mit einem QMS wird Sinnvoll

# Datensicherheitsmaßnahmen

- der § 14 DSG 2000 verpflichtet alle Organisationseinheiten eines Auftraggebers (Verantwortlichen) oder Dienstleisters (Auftragsverarbeiters), die Daten verwenden, dazu, Maßnahmen zur Gewährleistung der Datensicherheit zu treffen
- die DSGVO – Art 32 legt fest, dass der Verantwortliche ein angemessenes Schutzniveau zu gewährleisten hat

# Datensparsamkeit

- Sowohl der Grundsatz der Verarbeitung nach Treu und Glauben lt. Art 5 Abs 1a als auch der Grundsatz der Zweckbindung lt. Art 5 Abs 1b bedingen grundsätzliche Datensparsamkeit
- lt. Art 5 Abs 1c ist die Verarbeitung auf ein notwendiges Maß zu beschränken -  
**Datenminimierung**

# Datenübermittlung

- nach Art 30 hat der Verantwortliche und auch der Auftagsverarbeiter, Kategorien von Empfängern, aber auch Übermittlung von personenbezogenen Daten an ein Drittland oder internationale Organisationen in einem Verzeichnis zu führen.
- Das Verzeichnis muss der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden.

# Datenvorfall

- It Art 33 hat der Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen **72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Art 55 zuständigen Aufsichtsbehörde zu melden
- Diese erweiterten Melde- und Benachrichtigungspflichten benötigen eine **vertragliche Gestaltung durch eine „Data Breach Notification – Klausel“**

# Informationspflichten

- Im Rahmen der Informationspflicht - Art 13 u. Art 14 als auch im Auskunftsrecht – Art 15
  - die Verarbeitungszwecke; die Kategorien personenbezogener Daten, die verarbeitet werden; die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind
  - falls möglich die geplante Dauer oder falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
  - das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
  - wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten

# Verantwortlichkeiten

- „Accountability“ – „verschärfte Verpflichtungen“ des Verantwortlichen
- Selbstverantwortung - Verantwortlicher muss die Einhaltung der Grundsätze nachweisen können
- technische und organisatorische Maßnahmen regelmäßig überprüfen
- „Privacy by Design“ und „Privacy by Default“
- Datenschutzrichtlinie „Privacy Policy“

# Kontrollbereich RECHT 1/2

- Anwendungsbereich
  - Datenklassifizierung
- Betroffenenrechte
- Aufbewahrung von Daten
- Datenschutz-Folgeabschätzung
  - Maßnahmen
- Datenschutzkonzept und –maßnahmen
- Datenübermittlung
  - Genehmigung
  - Zulässigkeit

# Kontrollbereich RECHT 2/2

- Informationspflichten
  - Datenverarbeitung
  - Verfahren
- Rechtmäßigkeit
  - Datenklassifizierung
  - Einwilligung
  - Prüfpflichten
  - Zweckbindung
- Verantwortlichkeiten
  - Gemeinsame Datenverarbeitung

# Kontrollbereich PROZESS 1/3

- Anwendungsbereich
  - Datenklassifizierung
- Betroffenenrechte
  - Datensparsamkeit
  - Informationspflicht
  - Löschpflicht
  - Richtigstellungspflicht
  - Widerspruch
- Aufbewahrung von Daten

# Kontrollbereich PROZESS 2/3

- Datenschutzkonzept und –management
  - Dokumentation und Nachweis
- Datensparsamkeit
- Datenübermittlung
- Datenvorfall
  - Dokumentation
  - Mitteilungspflicht
- Informationspflicht
  - Widerspruchsrecht
  - Datenverarbeitung

# Kontrollbereich PROZESS 3/3

- Rechtmäßigkeit
  - Einwilligung
  - Prüfpflicht
- Verantwortlichkeiten
  - Datenverarbeitung

# Kontrollbereich ORGANISATION

- Datenschutzkonzept und –management
  - Datenschutzbeauftragter
  - Leitende Organe
  - Risikobewertung
  - Verschwiegenheit
- Verantwortlichkeiten
  - Auftragsverarbeitung
  - Datenverarbeitung

# Kontrollbereiche IKT 1/3

- Aufbewahrung von Daten
  - Aufbewahrungszeiten
  - Sperr- und Löschkonzept
  - Protokollierung (Logdaten)
- Datenschutzkonzept und –management
  - Richtlinien und Nachweise

# Kontrollbereiche IKT 2/3

- Datensicherheitsmaßnahmen
  - Aufgabenzuordnung und Belehrung
  - Risikobewertung
  - Datenklassifizierung
  - Zugriffskonzept
  - Netzwerksicherheit
  - Zutrittskonzept
  - Verfügbarkeit
  - Integrität
  - Speichersicherheit (CIA-Triade)
  - Performance
  - Kommunikationssicherheit (CIA-Triade)
  - Protokollierung

# Kontrollbereiche IKT 3/3

- Datensparsamkeit
- Datenübermittlung

# Was sind die nächsten Schritte?

- IKT-008: Sicherstellen von Protokollen
  - Ziel: durchgeführte Vorgänge pro Anwendung / Systemen / Netzwerk ... mittels Tool erfassen und analysieren
    - SIEM fasst Funktionen von Security Information Management (SIM) und Security Event Management (SEM) in einem Sicherheits-Management-System zusammen
    - Ein SIEM-System sammelt Protokolle und andere sicherheitsrelevante Dokumente für die Analyse.
  - Nachweis: Prozessbeschreibung, SOP,
    - Pro Projekt muss es ein AP geben, dass diesen Punkt behandelt
    - Pro Prozess muss der Grund für die Tätigkeiten beschrieben sein

**Welche Ziele wollen wir erreichen und  
worauf sollte noch geachtet werden**

# Maßnahmen gegen Angriffe

- PRÄVENTION
  - ist die Kombination aller eingesetzten Maßnahmen, die zum ERHALT der SCHUTZZIELE für die CIA-Triade dienen
- DETEKTIEREN
  - ist die Kombination aller eingesetzten Maßnahmen, die zum ERKENNEN von unerwünschten Abweichungen der SCHUTZZIELE der CIA-Triade dienen
- REAGIEREN
  - ist die Kombination aller Maßnahmen, die zum WIEDER-HERSTELLEN der SCHUTZZIELE für die CIA-Triade führen

# Welche Maßnahmen?

- Vorgangsweise:
  - Abgrenzen, damit abhängig vom Szenario die „richtigen“ Maßnahmen ausgewählt werden
  - Abgrenzen, damit abhängig von einer Risikoanalyse die „richtigen“ Maßnahmen ausgewählt werden
- Kernfrage:
  - Welche Maßnahmen sollen WANN in welcher REIHENFOGLE eingesetzt werden, um WELCHES Sicherheitsziel zu erreichen?

# IT-Risikomanagement

- Bereits zu Beginn der Digitalisierung wurde der aus dem betriebswirtschaftlichen Kontext bekannte Risikobegriff auf die Informations-technologie übertragen, die Teildisziplin des IT-Risikomanagements wurde abgeleitet.
- In der aktuelleren Literatur wird sehr oft von einem soziotechnischen System gesprochen<sup>1-4)</sup>

- 1) ISO/IEC 27000 Serie – Informationstechnik – IT-Sicherheitsverfahren –Informationssicherheits-Managementsysteme – Überblick und Terminologie
- 2) ISACA-Leitfaden IT-Risikomanagement – leicht gemacht mit COBIT. ISACA Germany Chapter
- 3) BSI – Bundesamt für Sicherheit in der Informationstechnik
- 4) Österreichisches Informationssicherheitshandbuch

# Compliance

- Ein allgemein anerkannte Definition des Begriffs „Compliance“ existiert nicht.
- Der Österreichische Corporate Governance Kodex definiert: „*Der Vorstand, die Geschäftsführung bzw. die Leitung hat für die Einhaltung der gesetzlichen Bestimmungen und unternehmensinternen Richtlinien zu sorgen*“

# IT-Compliance

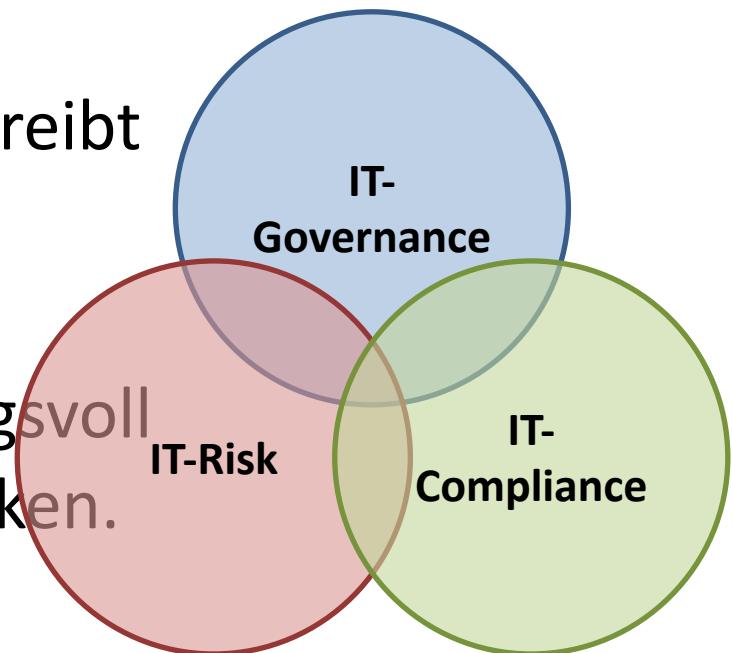
- IT-Compliance besteht aus 4 Komponenten:
  - Vorsorge gegen Gesetzesverstöße
  - Erfüllung von (branchenspezifischer) Vorgaben
  - Einführung eines IT-Risikomanagements sowie eines internen Kontrollsystems (IKS)
  - Persönliche Haftung des Managements bei Verletzung von Compliance-Vorgaben

# IT-GRC-Dreieck

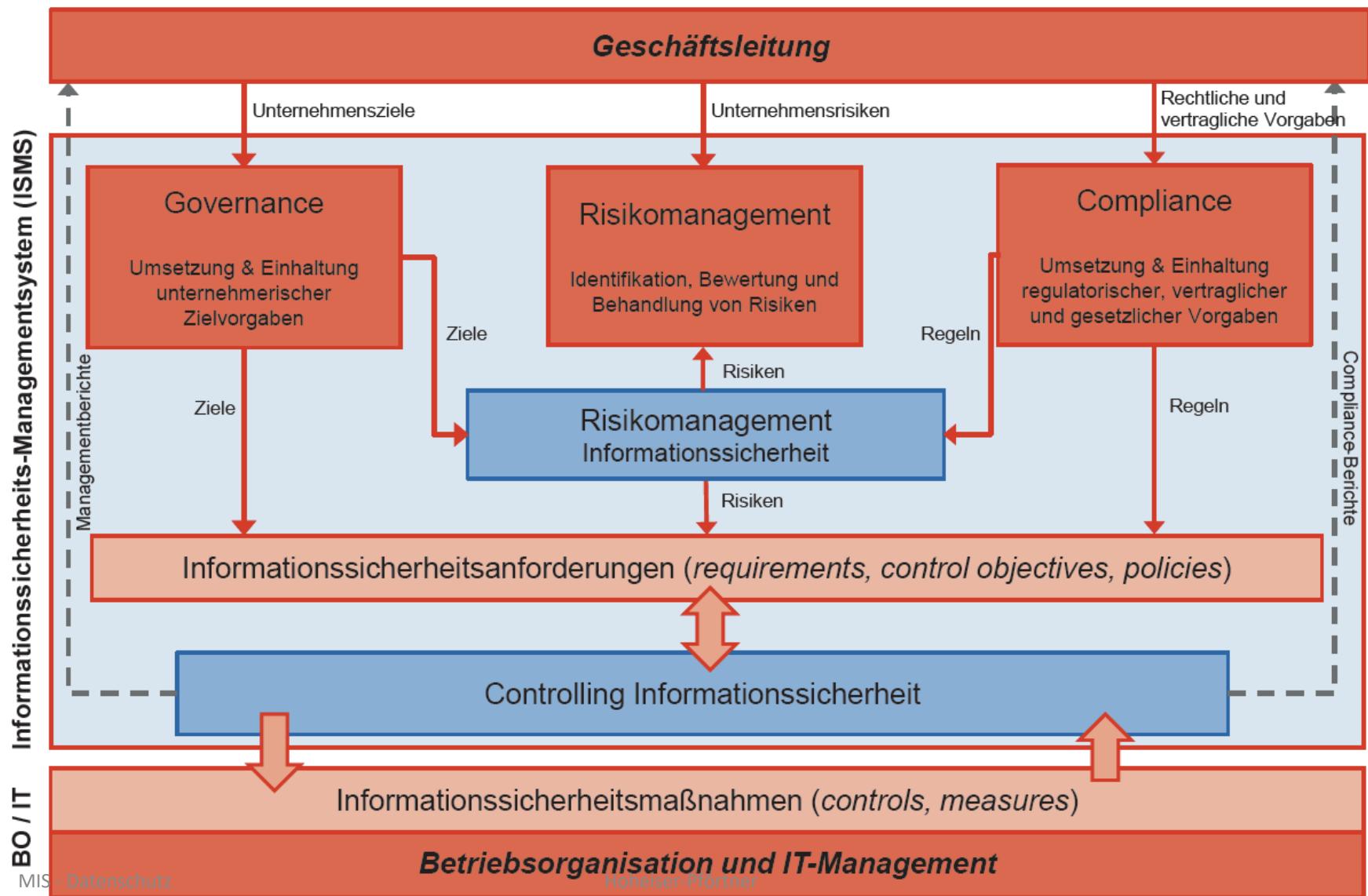
- Die Diskussion verdeutlicht, dass es ein Zusammenspiel zwischen IT-Governance, IT-Risikomanagement und IT-Compliance geben muss.
- Zwar lassen sich die Teildisziplinen voneinander unabhängig definieren und betrachten, sie sind aber nur gemeinsam in der Lage, Lösungen für die Herausforderungen der digitale Geschäftsprozesse zu entwickeln.

# IT-GRC-Dreieck

- IT-Governance achtet stets auf IT-Risiken und forciert IT-Riskomanagement und beschreibt alle Aspekte, die für die IT-Compliance notwendig sind.
- IT-Compliance schützt wirkungsvoll gegenüber bestimmten IT-Risiken.



# IT-GRC-Dreieck

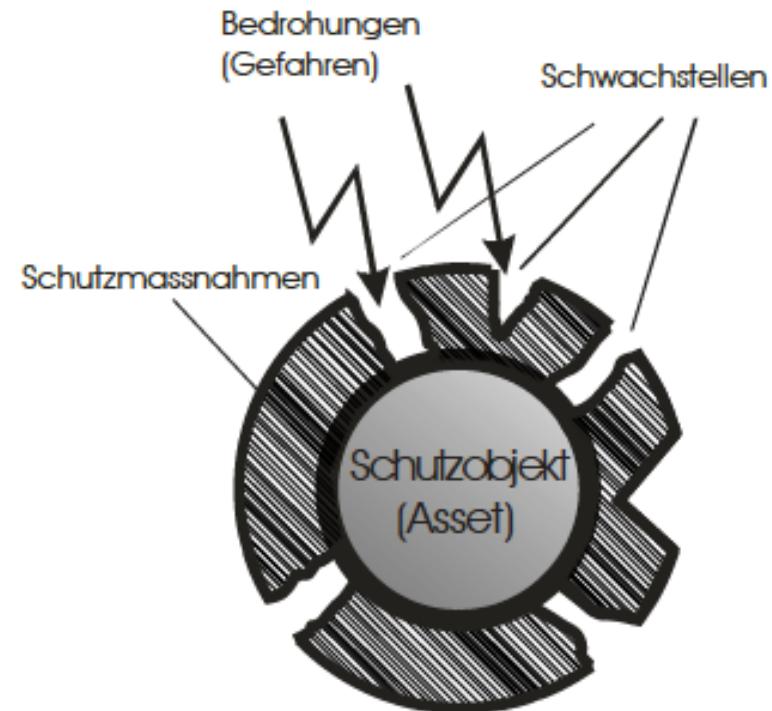


# Business Impact Analyse (BIA)

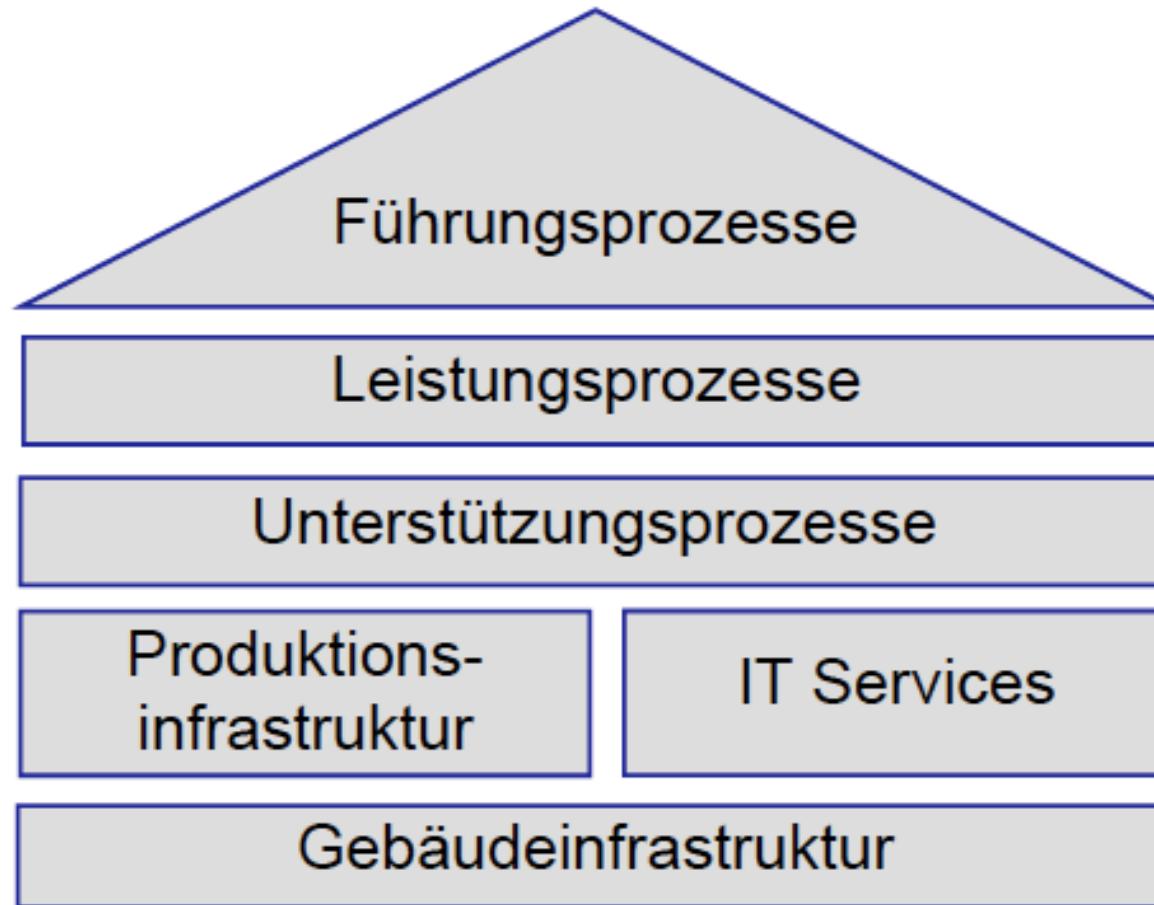
- Festlegen des Umfangs der BIA
- Konzeption der Impact Bewertung für die Verwundbarkeit der Vertraulichkeit, Integrität und Verfügbarkeit (CIA-Triade)

# Risiko bei Informationen

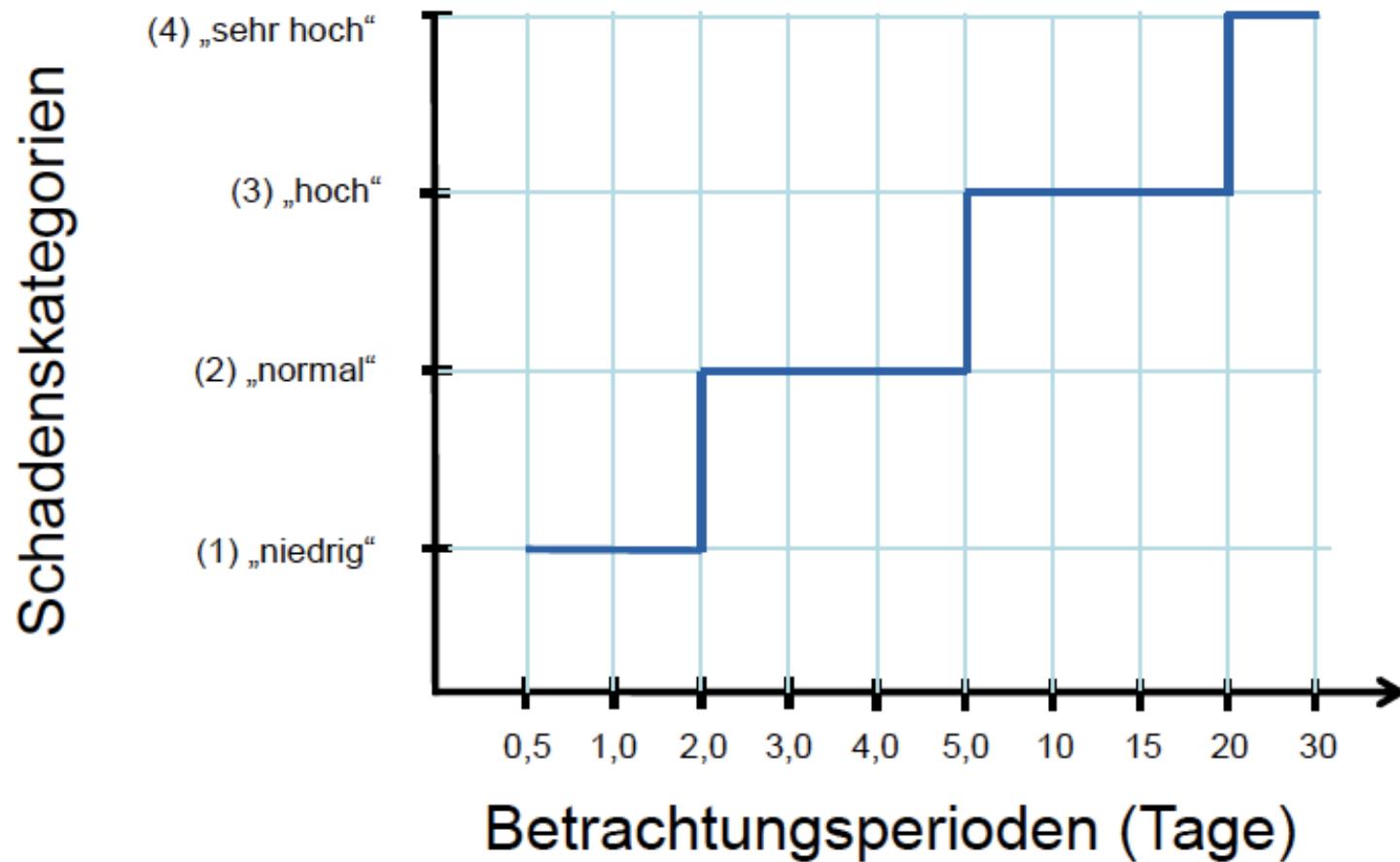
- Das Sicherheits-Risiko bei den Objekt „Informationen“ lässt sich aufgrund der drei folgenden Zielen bestimmen:
  - Vertraulichkeit
  - Integrität und
  - Verfügbarkeit



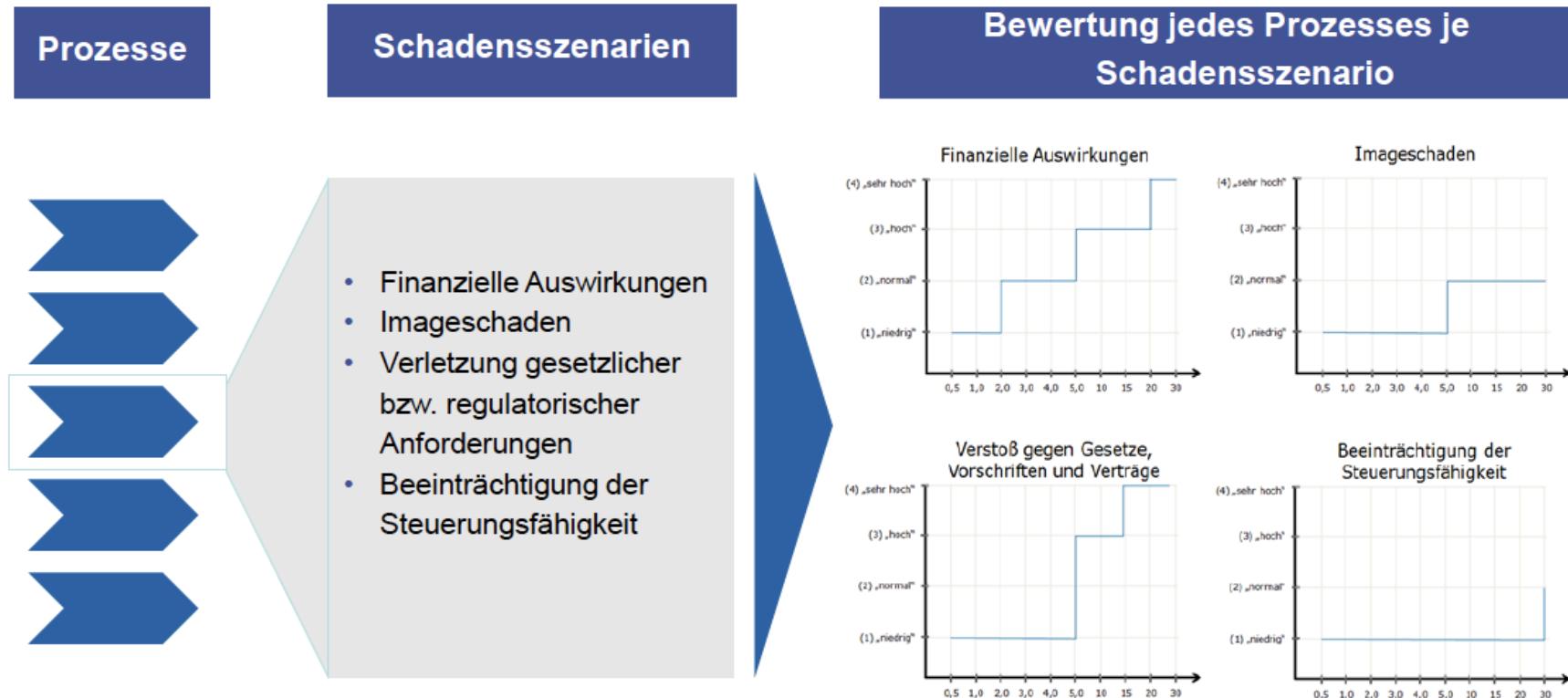
# Modellierung der Untersuchungsbereiche



# Betrachtungsperioden und Schadenskategorien



# Impact-Bewertung über 4 Szenarien



# Worauf sollten wir bei e-health Anwendungen achten?

# e-health Paradigmen

- Veränderte Strukturen im Gesundheitswesen und integrierte Versorgungsmodelle benötigen **IKT** für die Umsetzung
- Das Gesundheitswesen von „MORGEN“ ist:
  - patientenzentriert & benutzerorientiert
  - wissensbasiert
  - prozessorientiert
  - ergebnisorientiert
- Die integrierte Versorgung ist hierfür Schlüsselfunktion
  - vernetzen
  - kommunizieren
  - kooperieren

# integrierte Versorgung

- Verzahnung der Gesundheitsdiensteanbieter
  - Krankenhaus,
  - Hausarzt,
  - Labor,
  - Radiologie,
  - Mobile Krankenpflege, ...
- optimiertes Management entlang der Behandlungskette
- richtige Diagnose- & Therapieinformation zur richtigen Zeit am richtigen Ort
- Integration ist sektorübergreifend und schließt auch die behandelte Person mit ein „*m-Health / e-Health App*“

**Cybersecurity - Gestern, Heute & Morgen!**

## die Sicht der Hersteller

- Viele Medizinprodukte sind sicher, wenn sie einfach vom Netz abgesteckt werden
- Antivirus Software sowie Netzwerk „vulnerability scans“ können zeitkritische klinische Untersuchungen beeinflussen
- Medizinprodukte haben eine Lebensdauer von 10, 15, 20 und mehr Jahren
  - die IT-Betriebssystem haben eine viel **kürzere** Lebensdauer
- Authentifizierung von Benutzern muss „fail-open“ und nicht „fail-closed“ unterstützen

# die Sicht der Hersteller

- Viele Medizinprodukte sind sicher, wenn sie vom Netz abgesteckt werden
- Antivirus Software sowie Netzwerk „scans“ können zeitkritisch die Funktionen beeinflussen
- Medizinprodukte haben eine „Lebensdauer“ von 10, 15, 20 und mehr Jahren
  - die IT-Basis muss „fail-safe“ sein
- Authentifizierung muss „fail-open“ und nicht „fail-safe“ sein

**What do you mean by Fail-Open authentication?**

Fail-open authentication is the situation when the user authentication fails but results in providing open access to authenticated and secure sections of the web application to the end user.

# die Sicht der IKT im Spital

Mobilität & Zeitkritische Daten



Remote Services



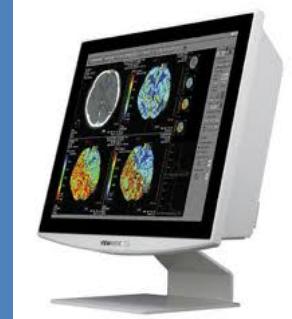
Notebook der Firmentechniker



Patch-management



Integration medizinischer Geräten im Netzwerk



Antivirus

Fehler im Netzwerk

Durchsatz im Netzwerk

Änderungen im Netzwerk

# die Sicht des Gesetzgebers

- Definition lt. Medizinproduktegesetz (MPG)  
**Medizinprodukt - „medizinische Geräte“**
  - alle einzeln oder miteinander verbundene Instrumente, Apparate, Vorrichtungen, Software, Stoffe oder andere Gegenstände samt Zubehör,
  - die zur Anwendung für diagnostische und/oder therapeutische Zwecke bestimmt sind
- oder vom Hersteller bestimmt sind
  - Erkennung, Verhütung, Überwachung, Behandlung, Linderung oder Kompensierung von Krankheiten, Verletzungen oder Behinderungen
  - Untersuchung, Ersatz oder Veränderung des anatomischen Aufbaus eines physiologischen Vorgangs, ...

# MPG: Verbote zum Schutz

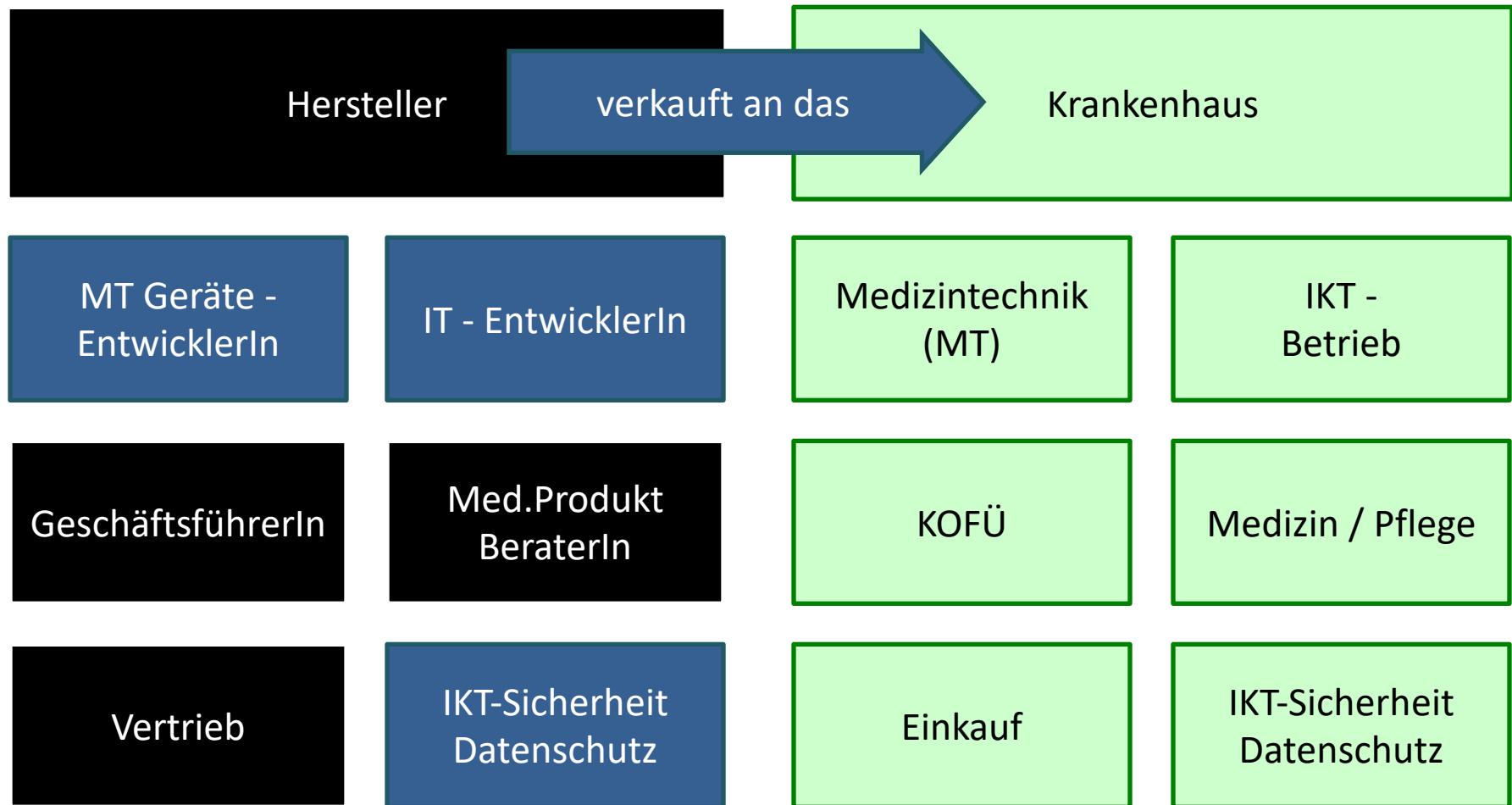
- Medizinprodukte herzustellen und einzusetzen, **wenn trotz sachgemäßer Anwendung**, Patienten oder Anwender gefährdet werden – unmittelbar oder mittelbar
- konstruktionsbedingte Sicherheit:
  - Beseitigen und minimieren von Risiken
  - Benutzer über Restrisiken unterweisen
  - Schutzmaßnahmen und Alarmfunktionen implementiert

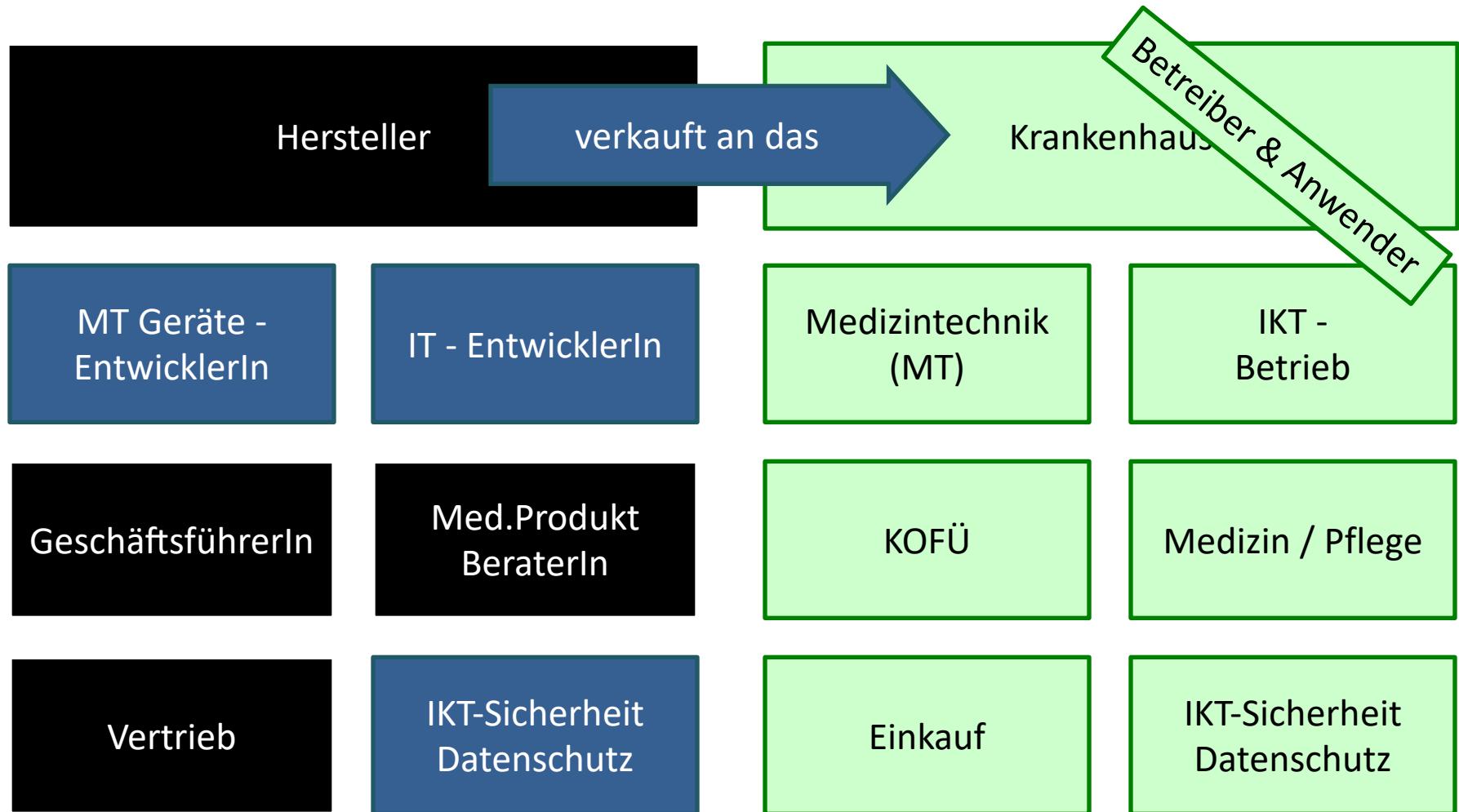
# was sagt die Normung

- EN ISO 14155: klinische Prüfungen medizinischer Produkten
- EN 1041: Informationen des Herstellers zu med. Produkten
- EN 1441: Risikoanalyse von medizinischen Produkten
- EN ISO 14971: Risikomanagement für med. Produkten
- EN 60601.1: Festlegung für die Sicherheit von med. Geräten
- EN 62304: Software Lebenszyklus für medizinische Produkte
- IEC 80001: Risikomanagement für med. Produkte in IT-Netzen
- ISO 27001: Informationssicherheit

# was wird wichtiger

- Die Vernetzung von medizinischen Geräten steigt und damit auch 3 wichtige Funktionen
  - gefahrloser Betrieb - **SAFETY**
  - sicherer Betrieb - **SECURITY**
  - wirksamer Betrieb – **EFFECTIVENESS**
- sowie 3 wichtige Aufgaben
  - die Integrationsprozesse ins IKT-Netzwerk sind definiert
  - die IKT-Risikomanagementprozesse sind etabliert
  - die Verantwortlichkeiten sind geklärt





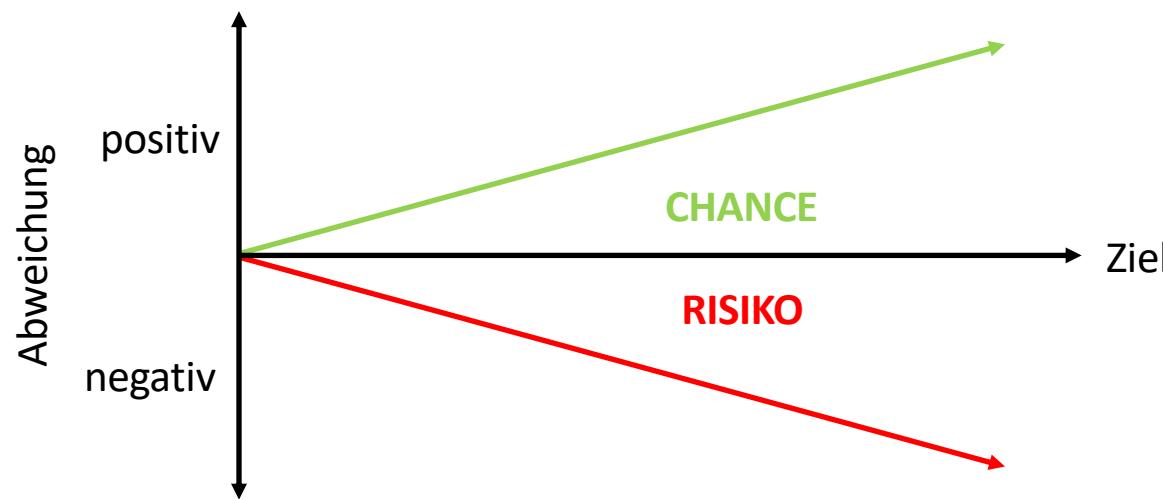
# Verantwortung

- **Hersteller**
  - liefert Daten zum Thema Risiko, Datenschnittstellen, ...
  - garantiert die Sicherheit seines Produktes nach IEC 60601
  - definiert die Zweckbestimmung seines Produktes
- **Betreiber**
  - setzt sich mit der Risikominimierung beim Integrationsprozess auseinander
  - übernimmt die Gesamtverantwortung
  - stellt den Behandlungsprozess, IKT-Sicherheit & Datenschutz
- **Anwender**
  - informiert über die kritischen Aspekte beim Behandlungsprozess
  - verwendet das Produkt entsprechend der Zweckbestimmung
  - kennt die Notfallpläne

# Warum ist eine gemeinsame Sicht wichtig?

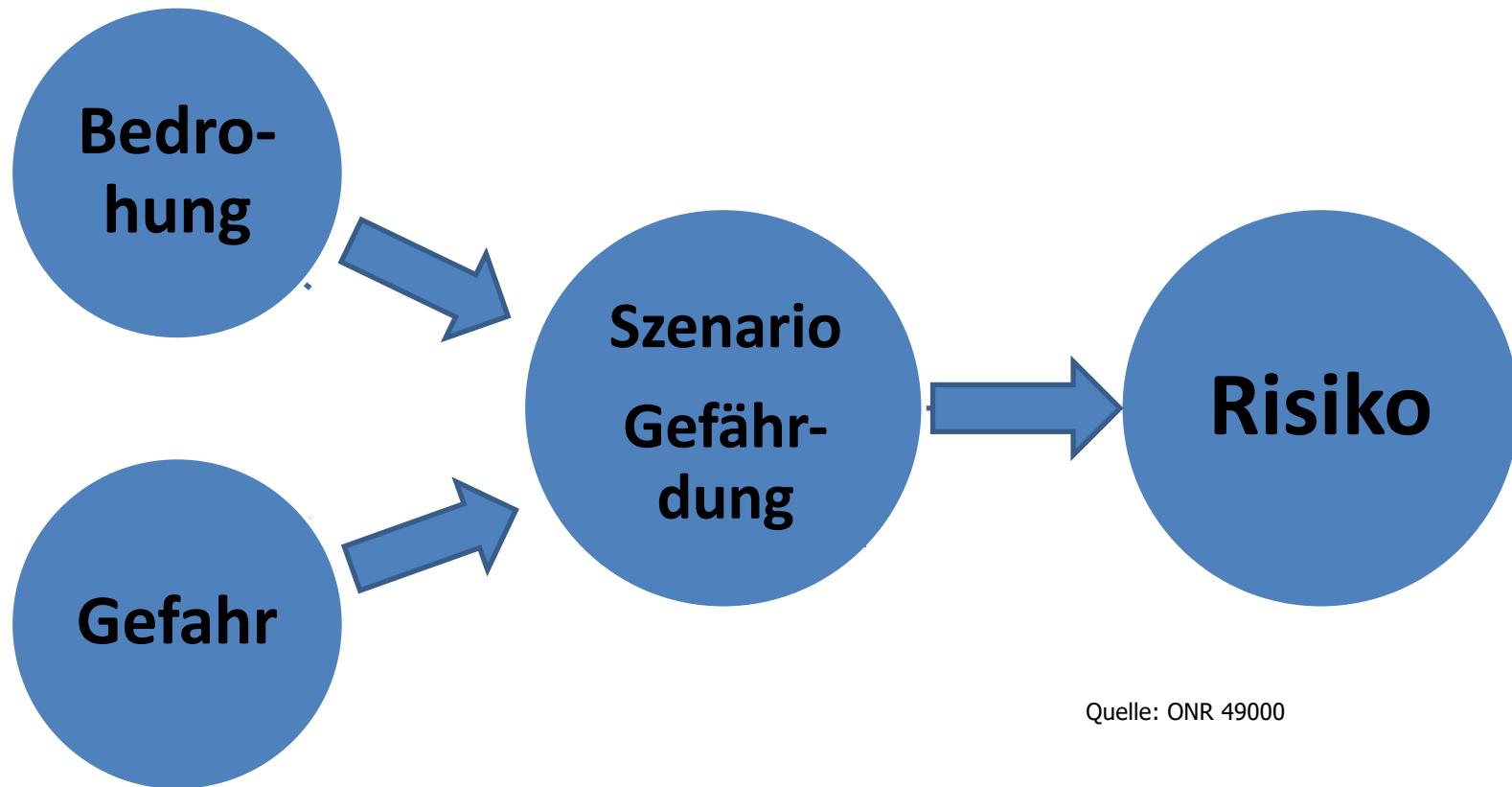
# Risiko : Chance

- unter dem Begriff Risiko versteht König:<sup>1)</sup>  
*“sowohl die positive als auch negative Abweichung eines definierten Ziels”*



1) Königs H-P (2017) IT-Risikomanagement mit System: Praxisorientiertes Management von Informationssicherheits- und IT-Risiken, 5. Aufl. Springer Vieweg, Wiesbaden

# Das Zusammenspiel beim Risiko



Quelle: ONR 49000

## IT-Risiko / Informationssicherheitsrisiko

- IT-Risiko geht einerseits eher von technischen Bedrohungen aus.
- Informationssicherheitsrisiko behandelt andererseits die Bedrohungen auf Geschäftsprozesse.
- Beide Sichtweisen haben ihre Berechtigung und sollten daher immer klargestellt werden
- Auswirkungen von IT-Risiken werden oft als Business Impact bezeichnet.

# IT-Risikomanagement

- Bereits zu Beginn der Digitalisierung wurde der aus dem betriebswirtschaftlichen Kontext bekannte Risikobegriff auf die Informations-technologie übertragen, die Teildisziplin des IT-Risikomanagements wurde abgeleitet.
- In der aktuelleren Literatur wird sehr oft von einem soziotechnischen System gesprochen<sup>1-4)</sup>

1) ISO/IEC 27000 Serie – Informationstechnik – IT-Sicherheitsverfahren –Informationssicherheits-Managementsysteme – Überblick und Terminologie

2) ISACA-Leitfaden IT-Risikomanagement – leicht gemacht mit COBIT. ISACA Germany Chapter

3) BSI – Bundesamt für Sicherheit in der Informationstechnik

4) Österreichisches Informationssicherheitshandbuch

# Risiko in der Med.-Technik

- Lt. ISO/IEC Guide 51 ist Risiko eine Kombination der Wahrscheinlichkeit des Auftretens eines Schadens und des Schweregrades dieses Schadens in der Zukunft
- Lt. ISO/IEC Guide 51 ist Schaden eine physische Verletzung oder Schädigung der menschlichen Gesundheit bzw. von Gütern oder Umwelt

## Schweregrad lt. EN ISO 14971

<b>Maß</b>	<b>Mögliche Folgen einer Gefährdung</b>
Katastrophal	Führt zum Tod des Patienten
Kritisch	Führt zu dauernder Behinderung oder einer lebensbedrohlichen Schädigung

## Schweregrad lt. EN ISO 14971

<b>Maß</b>	<b>Mögliche Folgen einer Gefährdung</b>
Ernst	Führt zu einer Schädigung oder Behinderung, die ein sachkundiges medizinisches Eingreifen erfordert

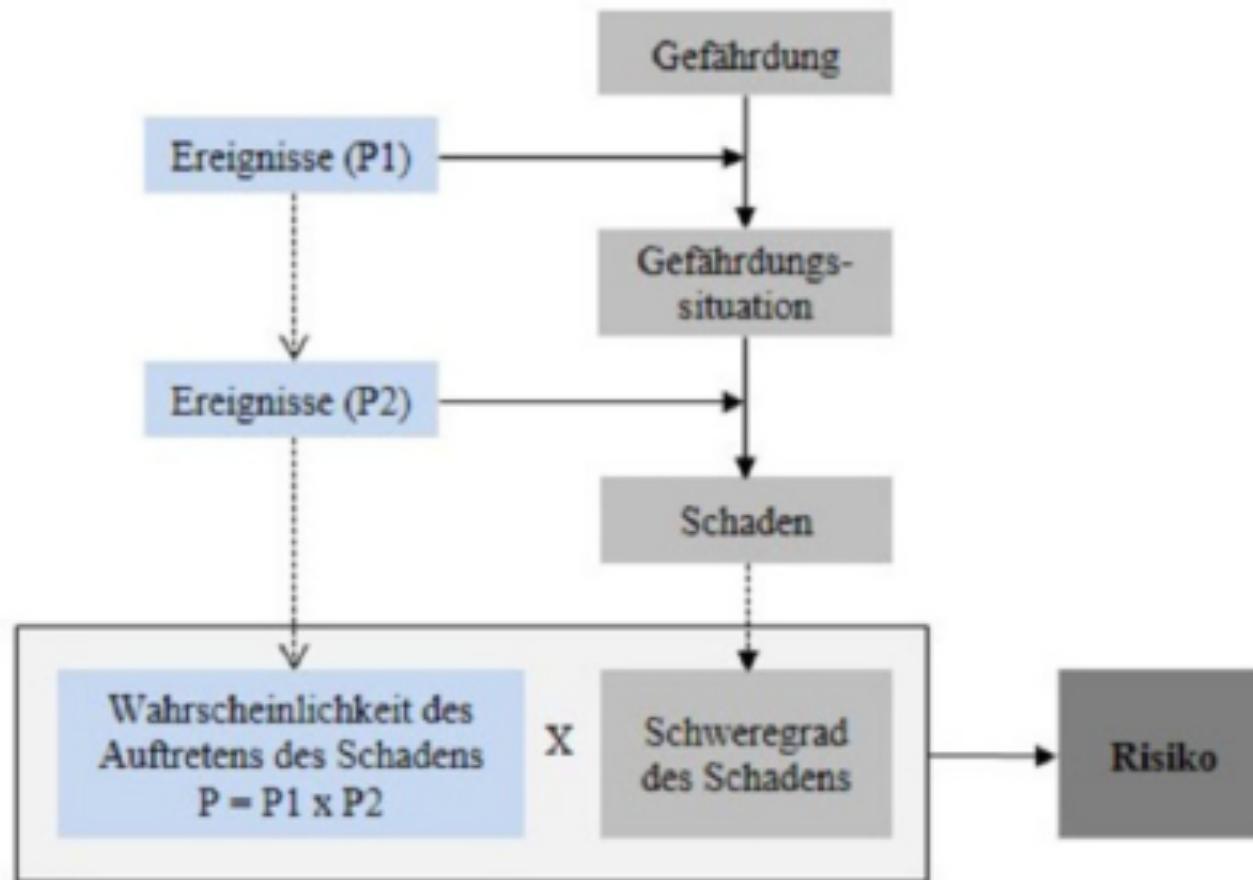
## Schweregrad lt. EN ISO 14971

<b>Maß</b>	<b>Mögliche Folgen einer Gefährdung</b>
Gering	Führt zu einer zeitweiligen Schädigung oder Behinderung, die kein sachkundiges medizinisches Eingreifen erfordert

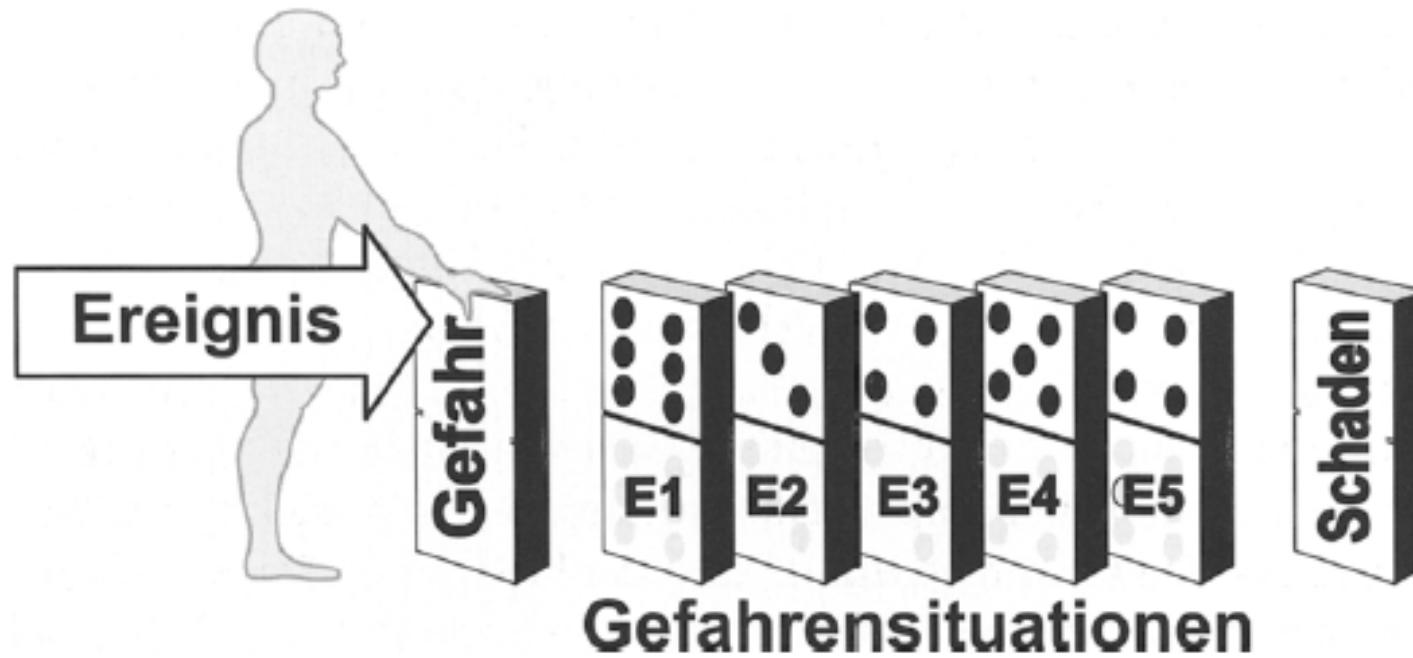
## Schweregrad lt. EN ISO 14971

<b>Maß</b>	<b>Mögliche Folgen einer Gefährdung</b>
Vernach-lässigbar	Unannehmlichkeiten oder zeitweilige Beschwerden

# Gefährdungssituation lt. EN ISO 14971



# Ereignisketten - Schaden



Quelle: Univ.-Prof. Dipl.-Ing. Dr. Norbert Leitgeb in  
Sicherheit von Medizingeräten

# Eintrittswahrscheinlichkeit lt. EN ISO 14971

## Bewertung der Eintrittswahrscheinlichkeit

häufig	$\geq 10^{-3}$		
wahrscheinlich	$< 10^{-3}$	und	$\geq 10^{-4}$
gelegentlich	$< 10^{-4}$	und	$\geq 10^{-5}$
fernliegend	$< 10^{-5}$	und	$\geq 10^{-6}$
unwahrscheinlich	$< 10^{-6}$		

# Risikobewertung lt. EN ISO 14971

Auftreten (A)	häufig $\geq 10^{-3}$	5	Schadensausmaß (B)			
	wahrscheinlich $< 10^{-3}$ und $\geq 10^{-4}$	4				
	gelegentlich $< 10^{-4}$ und $\geq 10^{-5}$	3				
	fernliegend $< 10^{-5}$ und $\geq 10^{-6}$	2				
	unwahrscheinlich $< 10^{-6}$	1				
			1	2	3	4
			ver-nach-lässig-bar	gering	ernst	kritisch
						Katas-trophal

# Risikomanagement ist

- die systematische **Erfassung** und **Bewertung** unternehmerischer Risiken
- entwickeln von **Strategien** zur Bewältigung dieser Risiken
- ein **permanente Aufgabe** in jedem Unternehmen
- Wegen seiner existentiellen Bedeutung bei der **Unternehmensleitung** angesiedelt

# Risikoanalyse ist

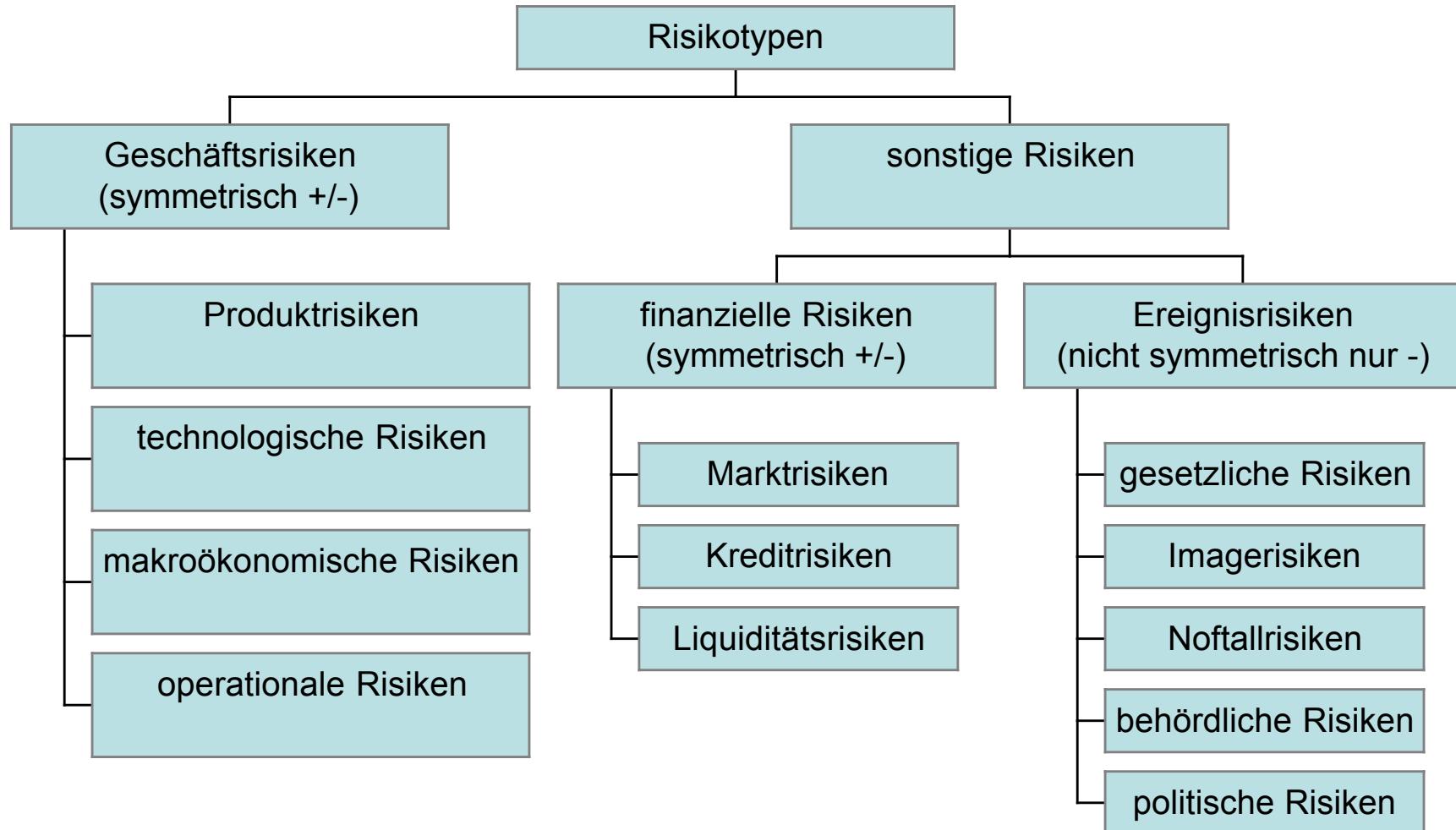
- die **Erfassung** von **Gefahren**<sup>1)</sup>
  - die **Ableitung** der **Risiken**
  - die **Klassifizierung** der **Risiken**
  - die **Bewertung** der **Risiken**
- 
- 1) **Gefahr** oder **Bedrohung** ist
  - das **Risiko** eines Feuers ist die **Wahrscheinlichkeit**, mit der das Feuer **eintritt** und der daraus resultierende **Schaden**

# Was soll man tun?

## einige Weisheiten zum Thema:

- **Zitat von Bruce Schneier:** (ein ‚Sicherheitspapst‘)
  - „The only secure Computer is one that's turned off, locked in a safe, and
    - buried 20 feet down in a secret location – and I'm not completely
      - confident of that one either”
  - Fazit: ist sowieso nichts zu machen, also Augen zu und durch?
- „Nein, halten wir uns lieber an Erich Kästner:
  - An allem Unfug, der passiert, sind nicht etwa nur die Schuld, die ihn tun,
    - sondern auch die, die ihn nicht verhindern!“
  - Fazit: wir sollten und wir können auch was tun, aber.....
- **Zitat von Joachim Ringelnatz:**
  - „Sicher ist, dass nichts sicher ist. Selbst das ist nicht sicher.“
  - Fazit: Perfekte Sicherheit ist nicht erreichbar, das ist ja normal

# Klassifizierung



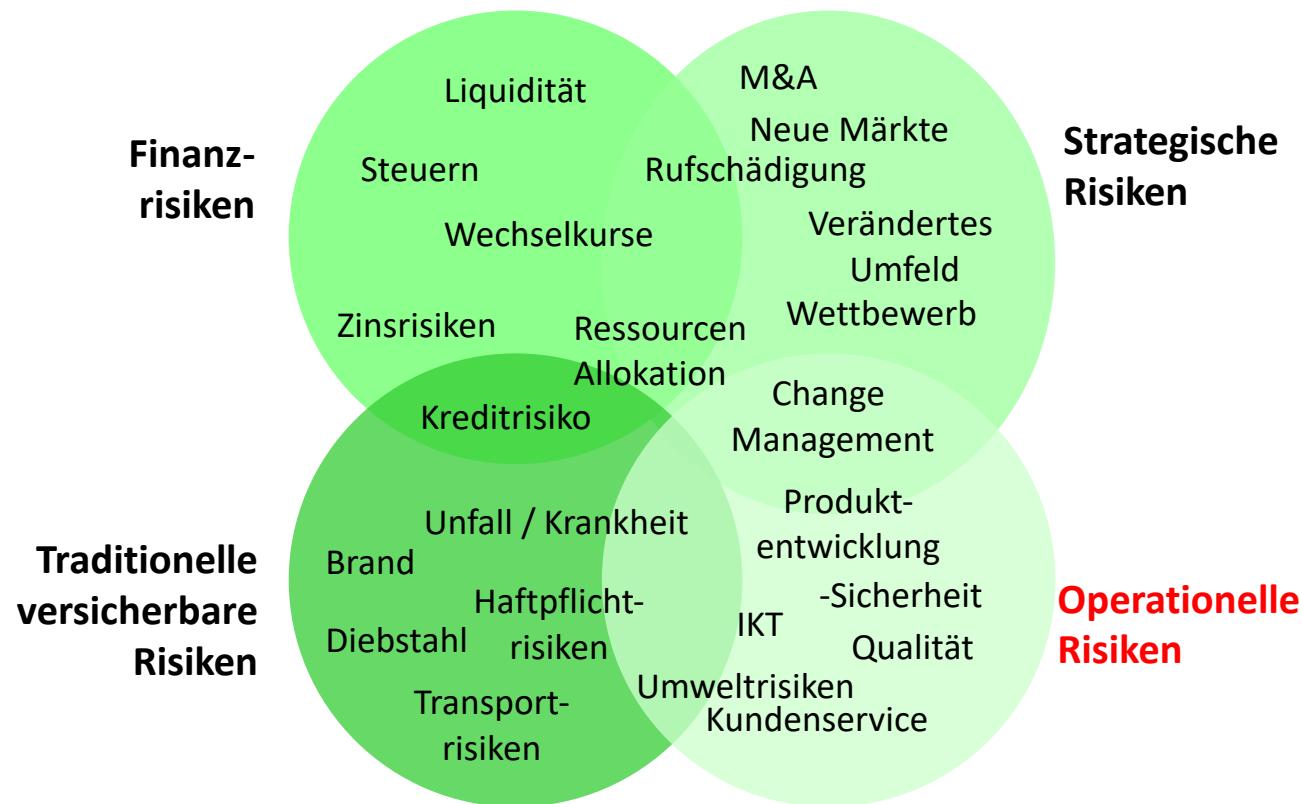
# RisikoMgmtProzess

- Der RisikoMgmtProzess ist ein kontinuierlich ablaufender Regelkreislauf aus den Kernelementen der Analyse, der Bewertung, der Handhabung und der Steuerung von Risiken.
- Dieser Kreislauf bildet den Kern des RisikoMgmtProzesses.

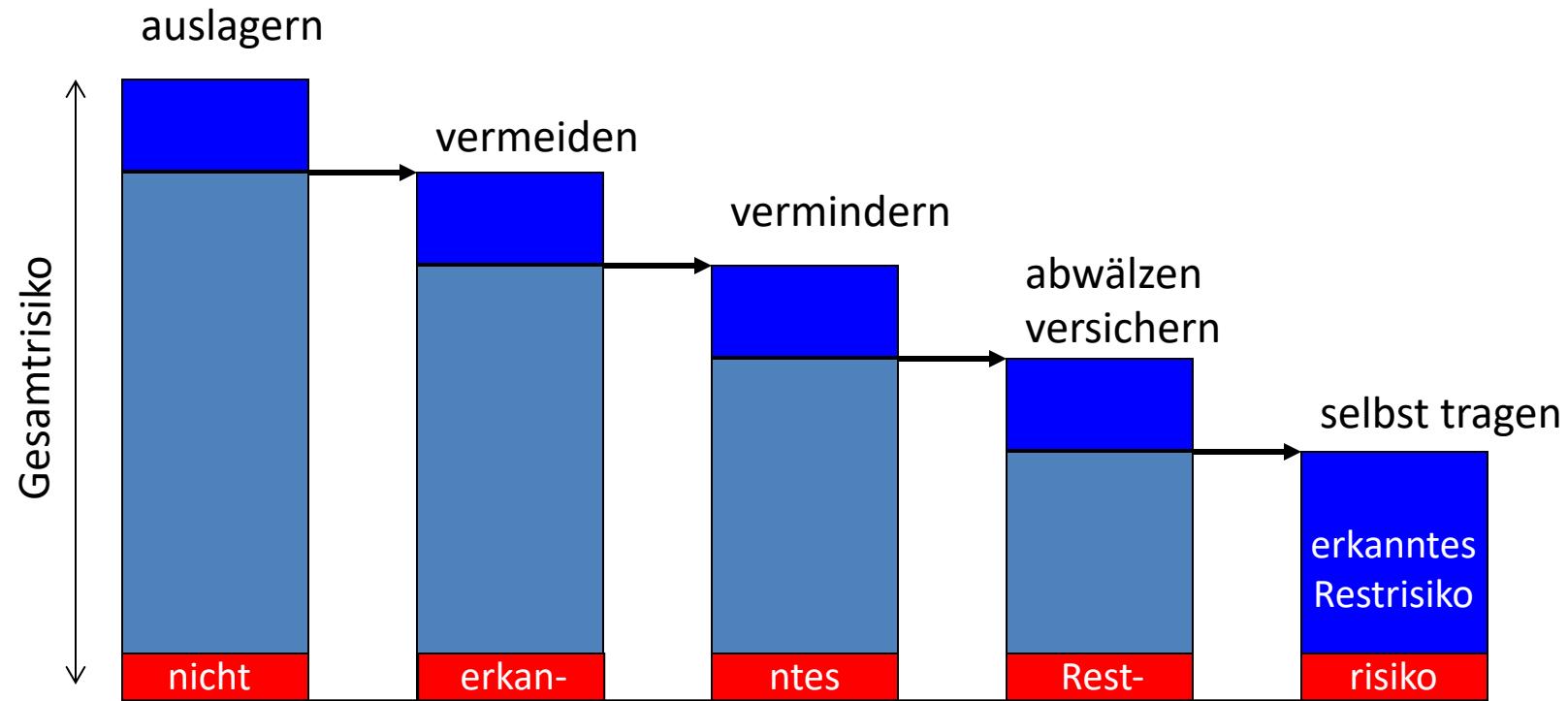
# Risikomanagement

- ... ist **keine** neue Erfindung.
- Unternehmerisches Handeln beinhaltet grundsätzlich Risiken
- der Umgang mit diesen Risiken ist Kern der unternehmerischen Tätigkeit
- Ein unternehmensweiter Ansatz des RisikoMgmt erfordert die umfassende Einführung neuer und die Integration bereits vorhandener RisikoMgmtSysteme sowie die Etablierung einer **Risikokultur**

# Welche Risiken auf ein tragfähiges Maß reduzieren?

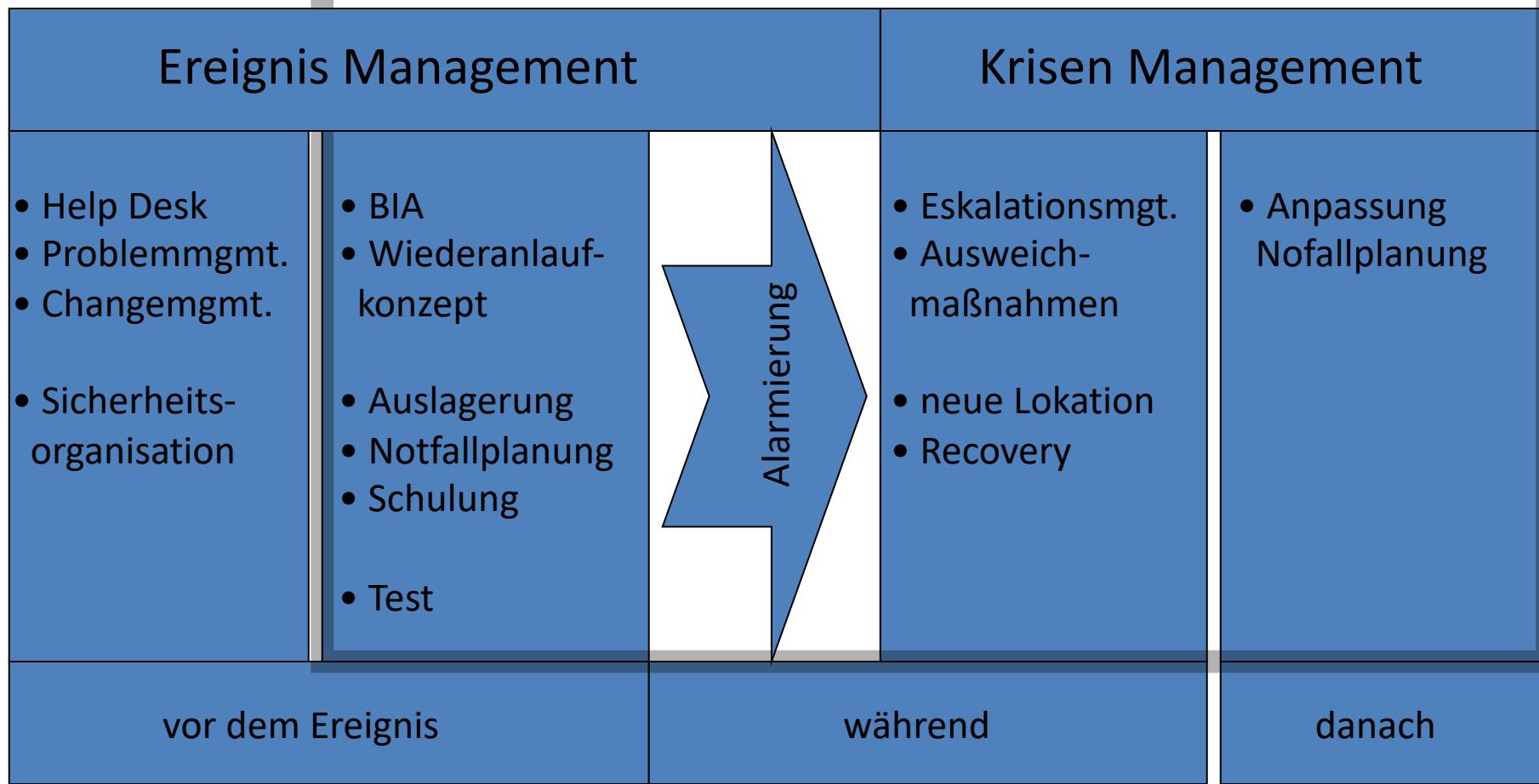


# Risikostruktur



# was ist Business Continuity

## Business Recovery

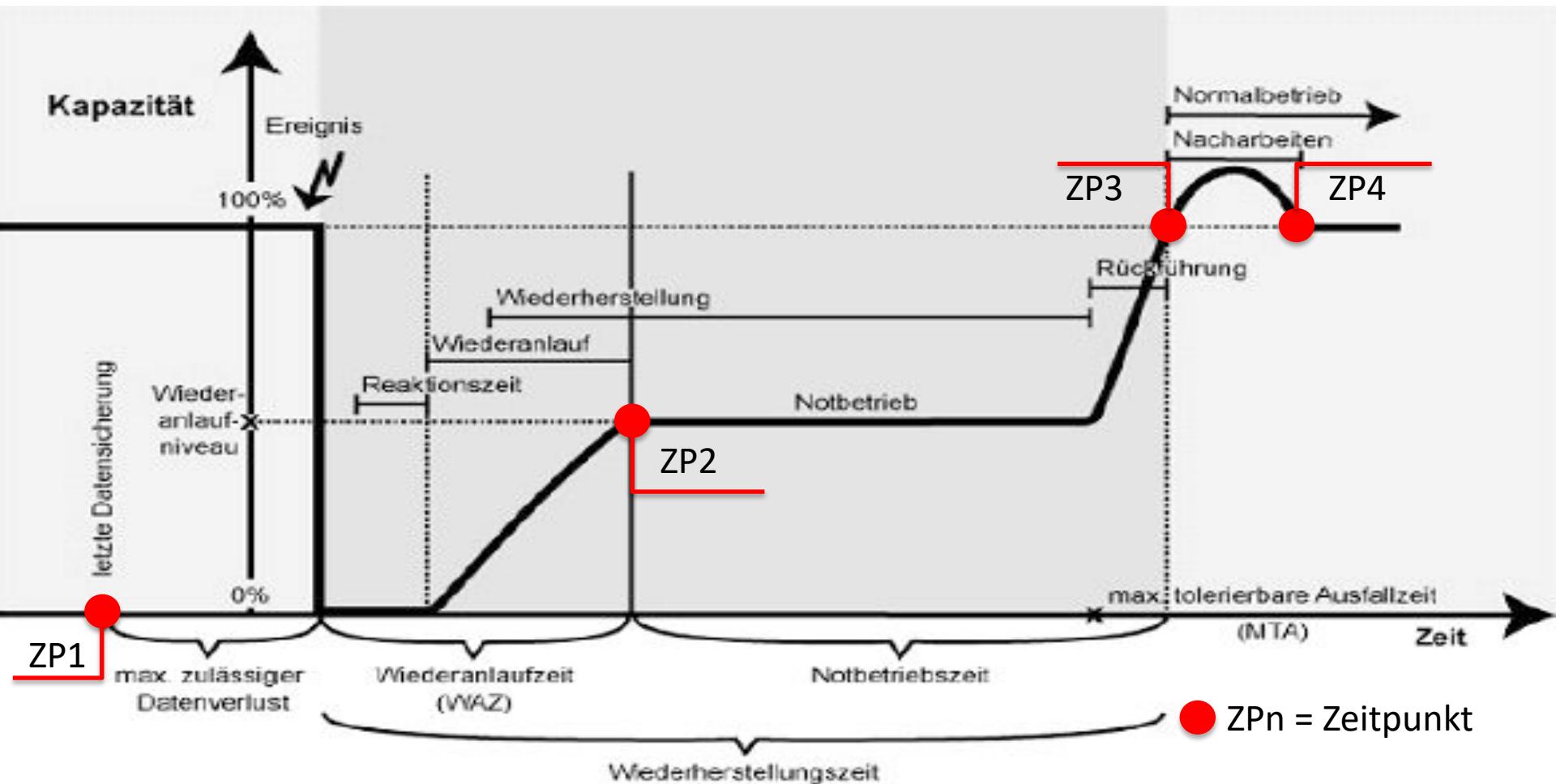


# Geschäftsprozess Sicherheit

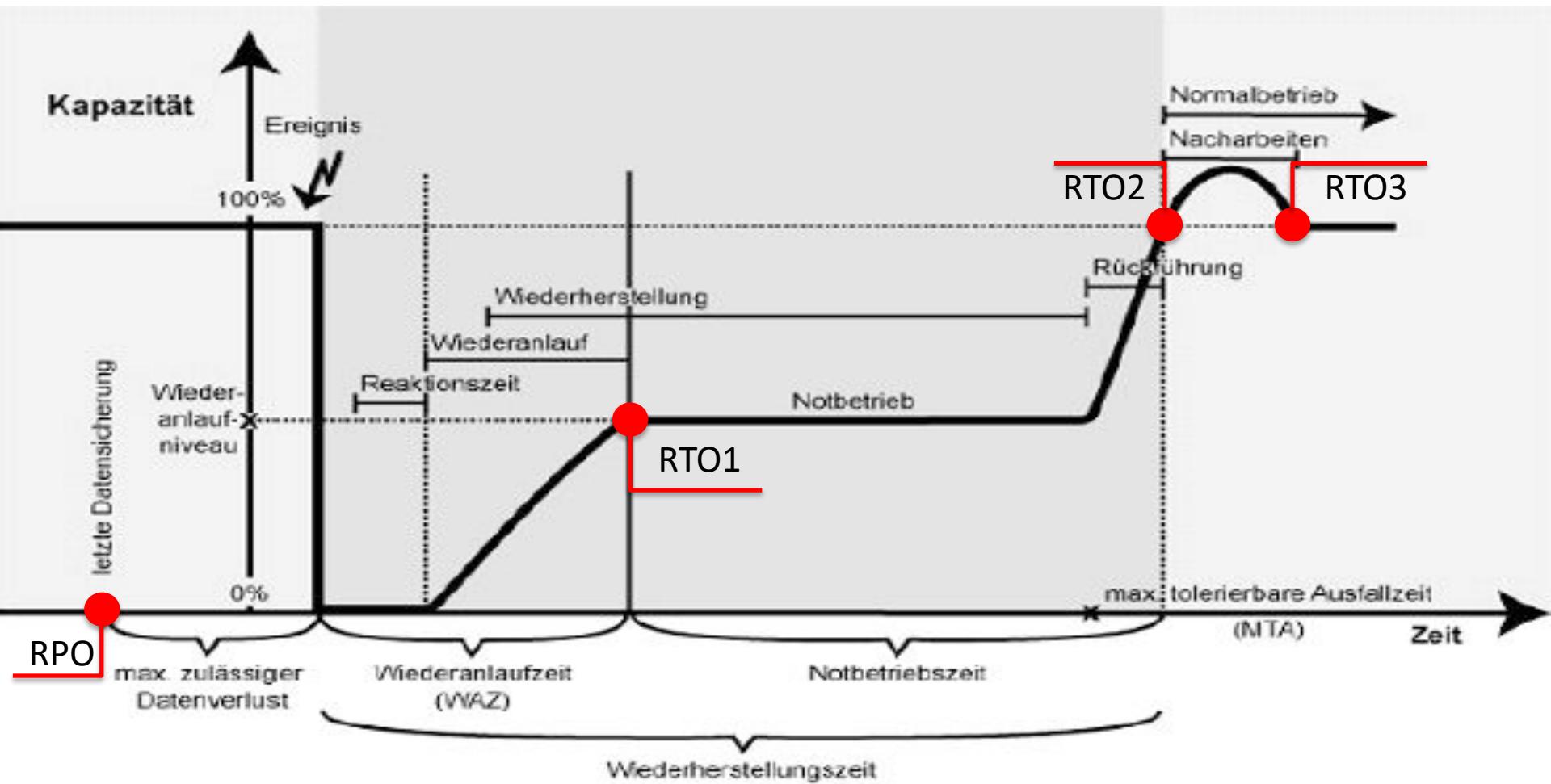
(Quelle E&Y)



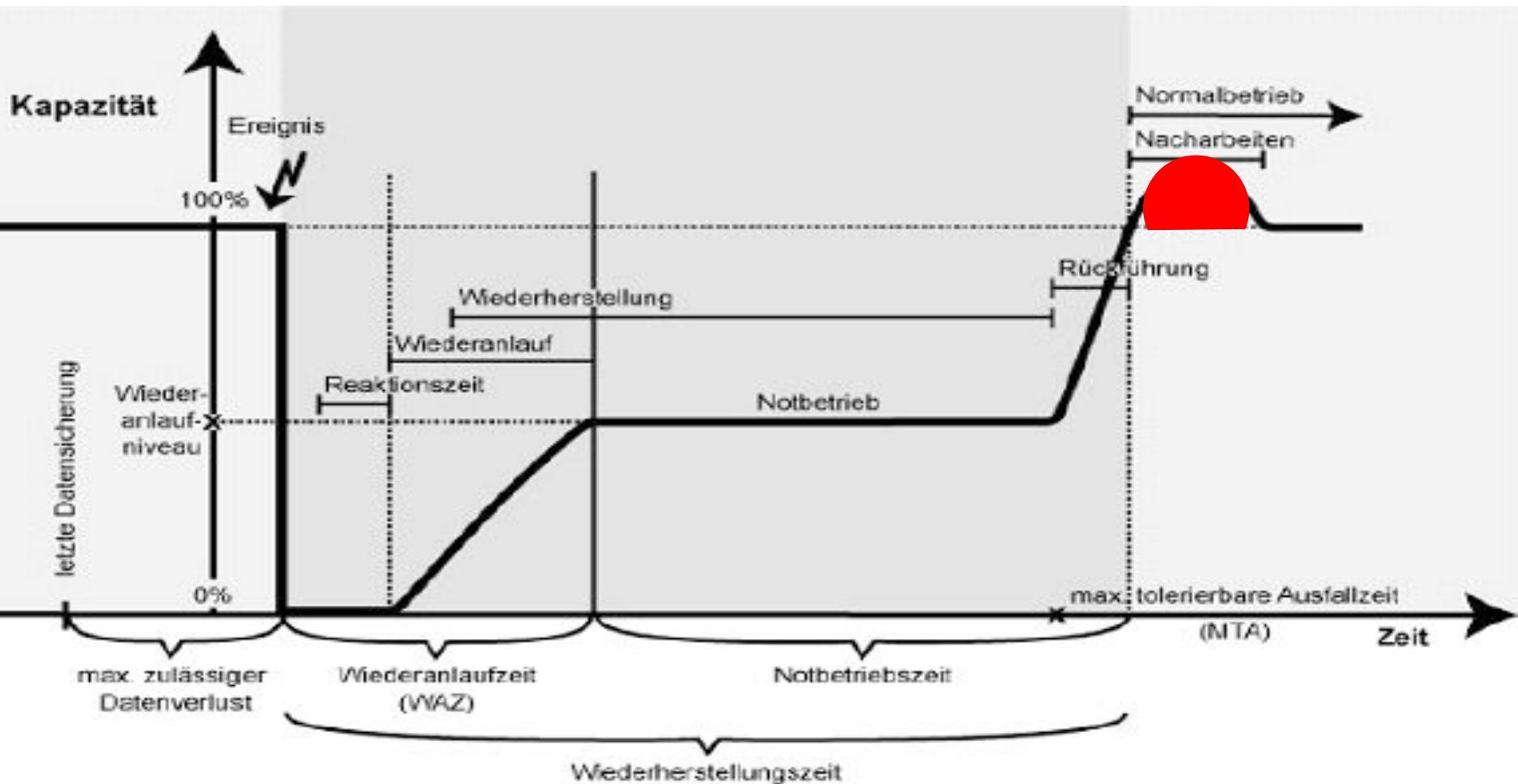
# Recovery POINT Objective & Recovery TIME Objective lt. BSI 100-4



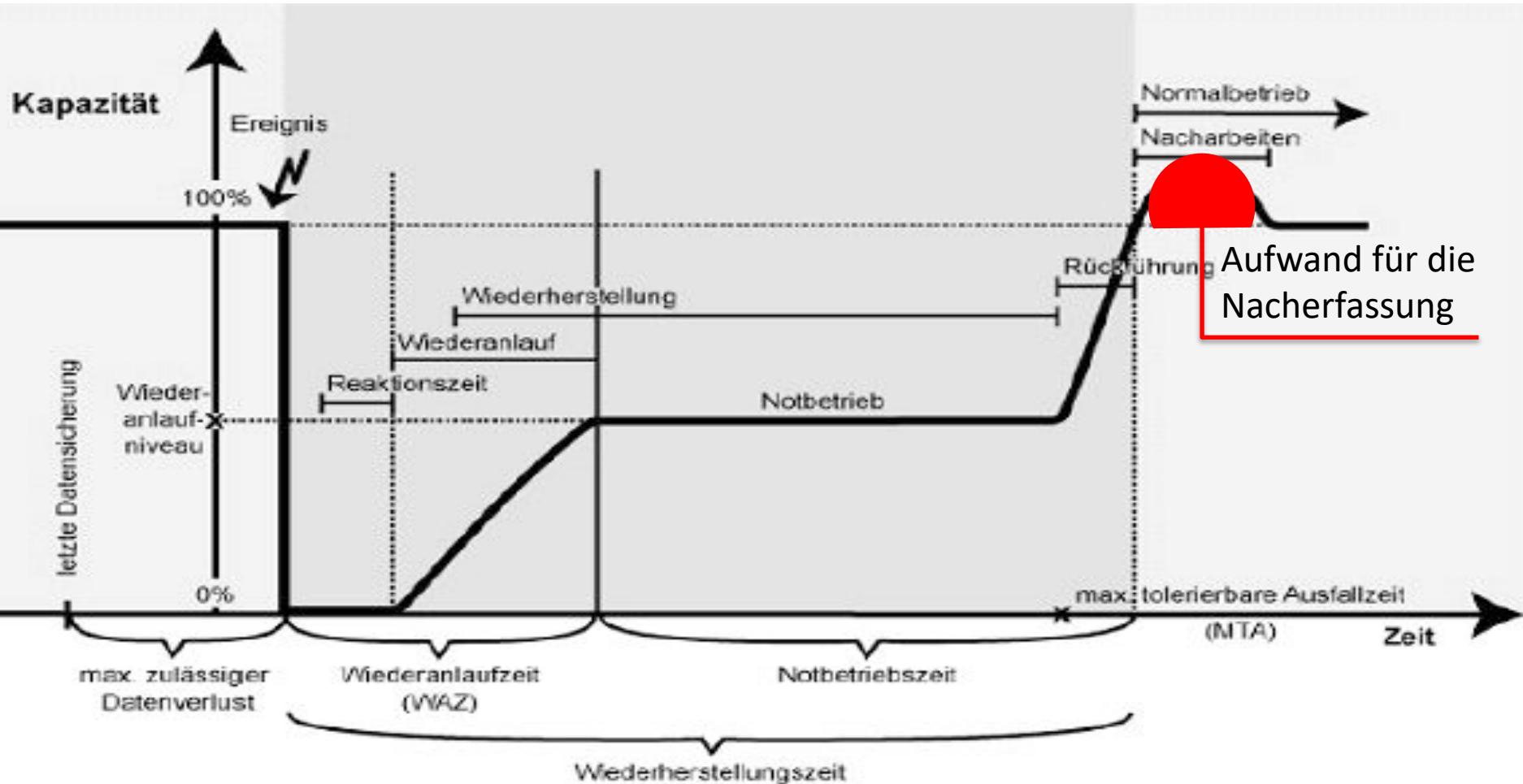
# Recovery POINT Objective & Recovery TIME Objective lt. BSI 100-4



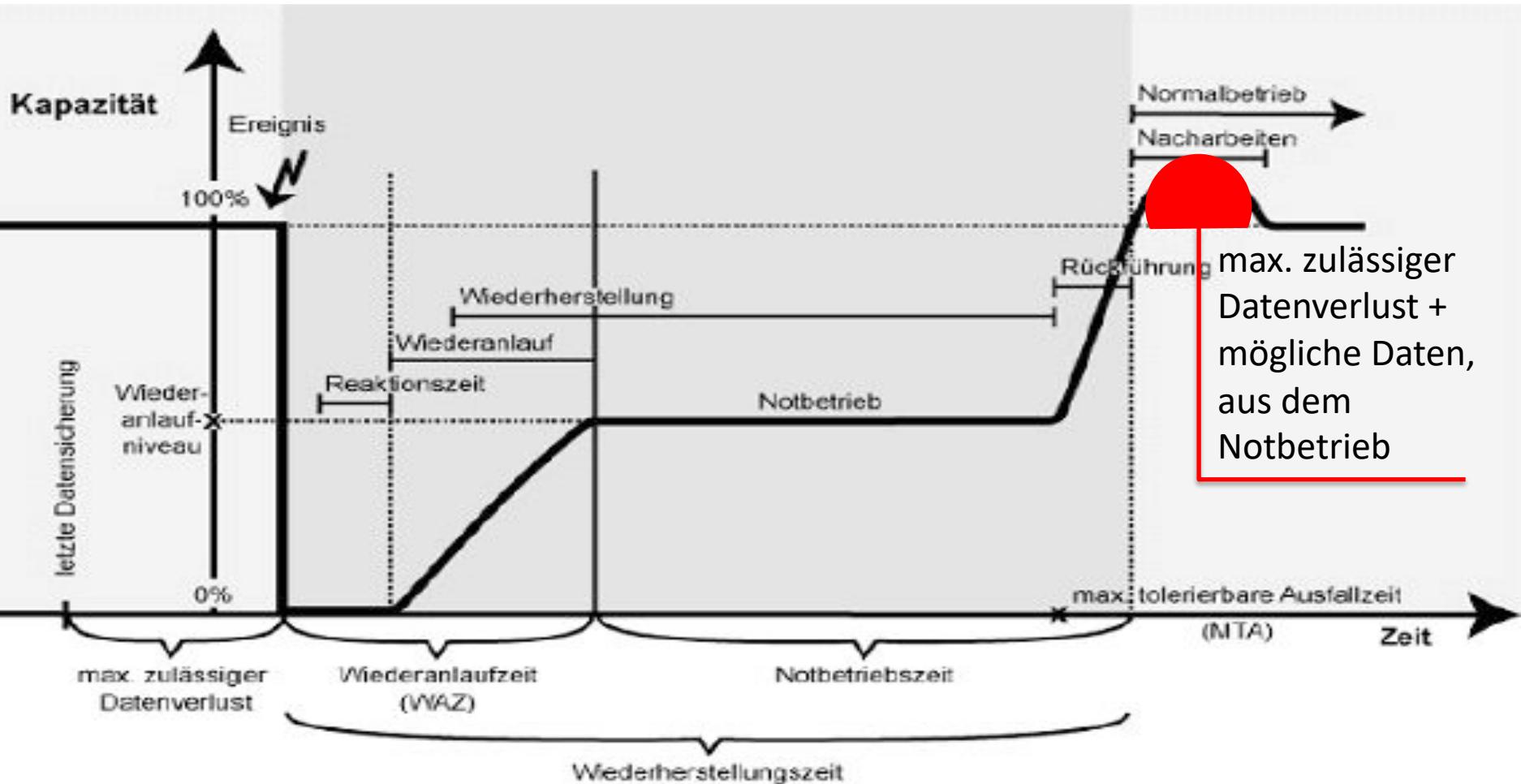
# Recovery POINT Objective & Recovery TIME Objective lt. BSI 100-4



# Recovery POINT Objective & Recovery TIME Objective lt. BSI 100-4



# Recovery POINT Objective & Recovery TIME Objective lt. BSI 100-4



# Notfallhandbuch / Notfallplan - Aufbau

- 1. Zweck des KAT- / Notfallplanes
  - Ausfall des Standorts oder der Infrastruktur
  - Ausfall der Informationstechnik
  - Ausfall des Personals
  - Ausfall von Dienstleistern
  - Geltungsbereich, alle Mitarbeiter

# Notfallhandbuch / Notfallplan - Aufbau

- 2. Alarmstufen
  - Störung / Notfall / Krise / Katastrophe

	Alarmstufe			Beispiel		
1		Grün	Normalbetrieb			
2		Gelb	Störung	<b>menschliche Gesundheit:</b> Verletzungen		oder Erkrankungen ohne Arbeitsausfall <b>finanzieller Schaden:</b> Kompensationsschaden > 2000 Euro <b>Umwelt:</b> minimale sanierbare Umweltschäden ohne Verstöße gegen die Gesetzgebung
					3	<b>menschliche Gesundheit:</b> Verletzungen oder Erkrankungen die den Ausfall mindestens eines Arbeitstages nach sich ziehen. <b>finanzieller Schaden:</b> > 10.000 Euro <b>Umwelt:</b> sanierbare Schäden ohne Verstöße gegen die Gesetzgebung
					4	<b>menschliche Gesundheit:</b> Teilinvalidität; Verletzung oder chronische Erkrankungen mit Spitalsaufenthalt bei mindestens 3 Personen <b>finanzieller Schaden:</b> > 200.000 Euro <b>Umwelt:</b> reversible Schäden mit Verstöße gegen die gesetzliche Gesetzgebung
					5	<b>menschliche Gesundheit:</b> Tod oder Totalinvalidität <b>finanzieller Schaden:</b> > 1.000.000 Euro <b>Umwelt:</b> irreversible Schäden mit Verstöße gegen die gesetzliche Gesetzgebung

# Notfallhandbuch / Notfallplan - Aufbau

- 2.2. Einsatzleitung
  - Person, Abkürzung, Rufnummern
- 2.3 Alarmierung

*“Alle Mitarbeiter des Krankenhaus XY , Alte Poststraße 149, 8020 Graz sind aufgefordert, jede Störung an **+43 316 5453 144** zu melden. Ist diese nicht erreichbar oder besteht ein eindeutiges notfallrelevantes Ereignis ist direkt ein(e) Notfallbeauftragte(r) zu alarmieren bzw. die externen Einsatzkräfte Rettung, Feuerwehr oder Polizei”*

- 3. Rechtsgrundlagen

# Notfallhandbuch / Notfallplan - Aufbau

- 4. Organisationsplan
  - Liste von Kontakt Personen, deren Funktion und Aufgabenbereich
- 5. Beschreibung des Krankenhauses XYZ
- 6. Besonderheiten des Krankenhauses XYZ
- 7. Schutzziele

<b>Übergeordnete Schutzziele</b>	<b>Definition</b>
Schutz des Patienten	Der Gesundheitszustand des Patienten darf sich durch Ausfälle und Störungen durch die IT im Krankenhaus XYZ nicht verschlechtern.

<b>IT-Schutzziele</b>	<b>Übergeordnetes Schutzziel</b>
Verfügbarkeit	Die Medizinische Versorgung muss aufrecht erhalten werden im Störfall.
Integrität	Verfälschung der Daten muss verhindert werden
Vertraulichkeit	Unberechtigte Personen dürfen nicht in Patientendaten Einsicht haben.
Informations- und Kommunikationstechnologien Hoheiser-Pförtner	Kommunikationsnetz muss aufrecht erhalten werden.

# Notfallhandbuch / Notfallplan - Aufbau

- 7.1 Kernprozesse
- 7.2 Sekundärprozesse
- 7.3 Tertiäre Prozesse

<b>Kernprozesse</b>	
Patientenaufnahme	
Diagnostik	
Medizin	
Psychotherapie	
Physiotherapie	
Pflege	
Entlassung	
<b>sekundäre Prozesse</b>	
Medikamentenversorgung	
Laborleistungen	
Speisenversorgung	
Wäscheversorgung	
Materialversorgung	
<b>tertiäre Prozesse</b>	
Personalmanagement	
Finanzmanagement	
Gebäudemanagement	
Informationstechnologie	
Öffentlichkeitsarbeit	

# **Notfallhandbuch / Notfallplan - Aufbau**

- 8 Organisation
- 8.1 Notfall Einsatzleitung
  - Definition und Arbeitsweise
  - Räumliche Koordinationsstelle
- 8.2 Notfall-Sofortmaßnahmen
- 8.2.1 Alarmierung

# Notfallhandbuch / Notfallplan - Aufbau

- 8.2.2 Totalausfall der Kommunikationsinfrastruktur

Nr.	Aktivität	Verantwortlich
1	Erkennen das die Telefoninfrastruktur ausgefallen ist; Meldung dm IT-Heldesk unter Einhaltung des Alarmierungsweges	Meldende Person
2	Verwendung von Melde-Laufzetteln für die interne Kommunikation	Stationsverantwortliche
3	Meldung über Gebäude-Lautsprecheranlage, SMS Alarmierung und Portal	IT-Helpdesk
4	Schadensbehebung	IT-Betrieb
5	Nach 5min einberufen Notfall-Einsatzstabs	IT-Betrieb, Pforte

- 8.3 Aufrechterhaltung des Geschäftsbetriebes

# Notfallhandbuch / Notfallplan - Aufbau

- 8.4 Rückführung in den Normalbetrieb
- 8.5 Gegenstände der Aufarbeitung
  - Dokumentation des Ereignisses zur Aufarbeitung und Vorlage beim Vorstand
- 8.6 Maßnahmen zur Koordinierung
  - Dokumentation des Ereignisses
  - Kommunikationspläne bei Ausfall der Telekommunikationseinrichtungen
  - ...

# Notfallhandbuch / Notfallplan - Aufbau

- 8.7 Logistische Maßnahmen
  - Räume und Ausrüstung

	Anforderungen	Wartung	Anzahl (+Backup)
Simkarten	2000 Minuten + 1000 SMS + 1 GB Data (monatlich)	Zweiwöchentlich zum testen, ob sie noch aktiv sind	16 + 4
Laptops	Netzwerkanschluss + WLAN Richtige E-Mail-Anwendungen und Browsers sollen installiert und konfiguriert werden.	Wöchentlich zum testen und aufladen	3
GSM-Modems	Data- und SMS-fähig	wöchentlich an den Laptops zum testen, Kurzmitteilung zum Testzwecken zum schicken	3
Handys	Wireless und GPRS fähig E-Mail-Anwendungen und Browsers	Funktionalität wöchentlich zum testen Aufladen und Ausschalten	13 + 7
Funkgeräte	VHF - Programmiert	Zweiwöchentlich testen: In unterschiedlichen Gebäudeteilen mit der Zentrale zu kommunizieren	15

# Notfallübung / Übungsplan

- **Ausgangsszenario**
  - Teilweiser Ausfall der Telekommunikationssysteme des Krankenhauses XYZ
  - Physikalische Abtrennung der Amtsleitung durch Bauarbeiten
  - Telekommunikationswege werden erheblich beeinträchtigt

# Notfallübung / Übungsplan

- **Auswirkungen**
  - Kontakt zu Rettungsorganisationen und Leitstellen auf dem üblichen Weg nicht mehr möglich
  - Es muss auf alternative Kommunikationswege zurückgegriffen werden
  - Einlieferung von Notfällen sowie die Organisation von Krankentransporten sind ebenso beeinträchtigt
  - Alarmierung von Ärzten und anderem für den klinischen Betrieb wesentlichem Personal kann nicht mehr über das an die Amtsleitung angeschlossene Paging-System erfolgen.

# Notfallübung / Übungsplan

- **Ziel der Übung**
  - Überprüfung der im Notfallplan festgehaltenen Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebes
  - Zeigen, ob die entsprechenden Maßnahmen den betroffenen Übenden ausreichend bekannt sind
  - Überprüfung ob vorhandene Maßnahmen im Notfall auch praktisch umgesetzt werden können
  - Zusätzlich können im Zuge der Übung auch fehlende neue Maßnahmen identifiziert werden

# Notfallübung / Übungsplan

- **Übungs-Setup**
  - Start: Samstag 13.12.2014 08:00
  - Ende: Sonntag 14.12.2014 um 08:00
  - Hauptfokus: Notfallambulanz
  - Geplante Zeitpunkt der Übung darf nur dem Management des Klinikums sowie der Übungsleitung selbst bekannt ist.
  - Den von der Übung betroffenen Personal ist lediglich die Kalenderwoche, in welcher die Übung stattfindet, bekannt zu geben
  - → möglichst realistische Ausgangsbasis für die Übung

# Notfallübung / Übungsplan

- **Übungsrollen**
  - Übungsleitung
    - gesamte Organisation der Übung (Planung, Durchführung, Nachbearbeitung)
  - Übende
    - Personal der Notfallambulanz (Ärzte, Schwestern, Reinigungspersonal, etc.) inkl Einsatzleitung

# Notfallübung / Übungsplan

- **Übungsrollen**
  - Beobachter
    - Primäre Aufgabe: Aktivitäten der Übenden protokollieren für die spätere Auswertung
  - Beteiligte
    - jene Personen die nicht unmittelbar an der Übung beteiligt sind, aber dennoch über deren stattfinden informiert werden müssen (z.B. Leitstelle und Rettungsorganisationen)

# Notfallübung / Übungsplan

- **Kennzeichnung (mittels Westen)**

Rolle	Kennzeichnung	Berechtigung
Übungsleitung	gelb	dürfen Übenden Anweisungen geben bzw. über eingespielte Ereignisse informieren
Beobachter/ Beteiligte	grün	keine Kommunikation mit den Übenden

# Notfallübung / Übungsplan

- **Ablauf (Startphase)**
  - 13.12.2014 um 07:00: Übungsleitung informiert die betroffene Leitstelle sowie Rettungsorganisationen
  - (Durchführung der Übung wurde diesen Institutionen bereits im Vorfeld kommuniziert)
  - Notfälle werden alternative Kliniken/Ambulanzen im Einzugsgebiet umgeleitet
  - Techniker der IT-Abteilung trennt um 07:45 die Notfallambulanz von der Amtsleitung
  - 08:00 Briefing der Übungsleitung → offizieller Start der Übung

# Notfallübung / Übungsplan

- Übung durchführen

Ablaufplan Übung "Surdus"						
Zeit	Geplant	Code	Ereignis	Code	Einspielung	Code
8:00			Abtrennung Amtsleitung	E001		
9:00					Patienteneinlieferung mit Epidemieverdacht	S001
10:00			Ausrufung Krisenstab gemäß Notfallplan	E002		
11:00						
12:00					Verzögerung Anlieferung Organ	S002
13:00	Anlieferung Organ für Transplantation	P0 01				
14:00						
15:00						
16:00						
17:00						
18:00						
19:00						
20:00					Presse-Interview	S003
21:00						
22:00	Schichtwechsel	P0 02				
23:00						
0:00						
1:00						
2:00						
3:00						
4:00						
5:00						
6:00						
7:00						
8:00						

# Notfallübung / Übungsplan

## ■ Weitere geplante Einspielungen

A	B	C
Zeitpunkt <b>13:00</b>	GEPLANT	P001
<b>Kurztext:</b> Anlieferung Organ für Transplantation	<b>Langtext:</b> In der OP-Abteilung des Klinikums ist eine Organtransplantation im Verlauf des Nachmittags geplant. Der exakte Termin für die OP richtet sich nach dem Termin der Anlieferung.  Die Koordination und Organisation der Anlieferung des Organs erfolgt über die Notfallambulanz und wurde am Vortag folgendermaßen geplant: - Anlieferung VIE 11:00 - von dort per Krankentransport zur Notfall-Ambulanz des Klinikums  Für eine erfolgreiche OP muss das Organ in gutem Zustand sein, d.h. der Transport darf nicht zu lange dauern. Die Anlieferung muss daher bis spätestens 15:00 erfolgen.	

# Notfallübung / Übungsplan

## ■ Weitere geplante Einspielungen

Zeitpunkt	EINSPIELUNG	
9:00		S001
<b>Kurztext:</b>		
Patienteneinlieferung mit Epidemieverdacht		
<b>Langtext:</b>		
Ein kaum ansprechbarer Patient mit akuten Symptomen wird von einem Rettungsdienst in die Notfallambulanz eingeliefert.		
Der Patient kann zu seinen Symptomen keine Rückmeldung geben und ist kaum ansprechbar. Der Rettungsdienst berichtet jedoch, dass der Patient bei dessen Abholung über akutes Fieber, Schüttelfrost, Kopfschmerzen und Muskelschmerzen klagte. Ebenso sei der Patient vor ca. 2 Wochen von einer 3 monatigen Reise von Sierra-Leone zurück gekehrt. Es besteht somit der dringende Verdacht auf Ebola. Für die Rücksprache, Abklärung und Meldung des Verdachts gemäß Epidemiegesetz mit den zuständigen Behörden stehen die gewohnten Kommunikationswege aufgrund der szenarienbedingten Gegebenheiten nicht zur Verfügung.		

# Notfallübung / Übungsplan

- Weitere geplante Einspielungen

A	B	C
Zeitpunkt <b>10:15</b>	EINSPIELUNG	S003
Kurztext: Presse-Interview		
<u>Langtext:</u> Die Information über den Ebola-Verdachtsfall ist an die Presse gedrunnen.  Da die Pressestelle des Klinikums über die offiziellen Kommunikationskanäle nicht erreichbar ist, hat sich eine Schar von Journalisten namhafter Medien gleich direkt vor dem Krankenhaus eingefunden, um aktuelle Informationen zu erhalten. Die Neugier der Journalisten beeinträchtigt teilweise den Betrieb der Notfallambulanz. Wird die Journalistenschar nicht entsprechend abgefertigt, besteht zusätzlich die Gefahr der Verbreitung falscher Informationen und Panikmache.		

# Notfallübung / Übungsplan

- **Übungsauswertung**
  - Auswertung der Beobachterprotokolle
  - Erstellung eines detaillierten Berichtes
  - Kurzfassung wird an das Management geschickt
  - Langfassung geht an die Einsatzleitung
  - Bericht soll Aufschluss über etwaige fehlende Maßnahmen und möglichen Verbesserungspotentiale enthalten
  - inkl. kritischer Reflexion des Ablaufs der gegenständlichen Übung, welche als Lessons-Learned für zukünftige Übungen herangezogen werden soll

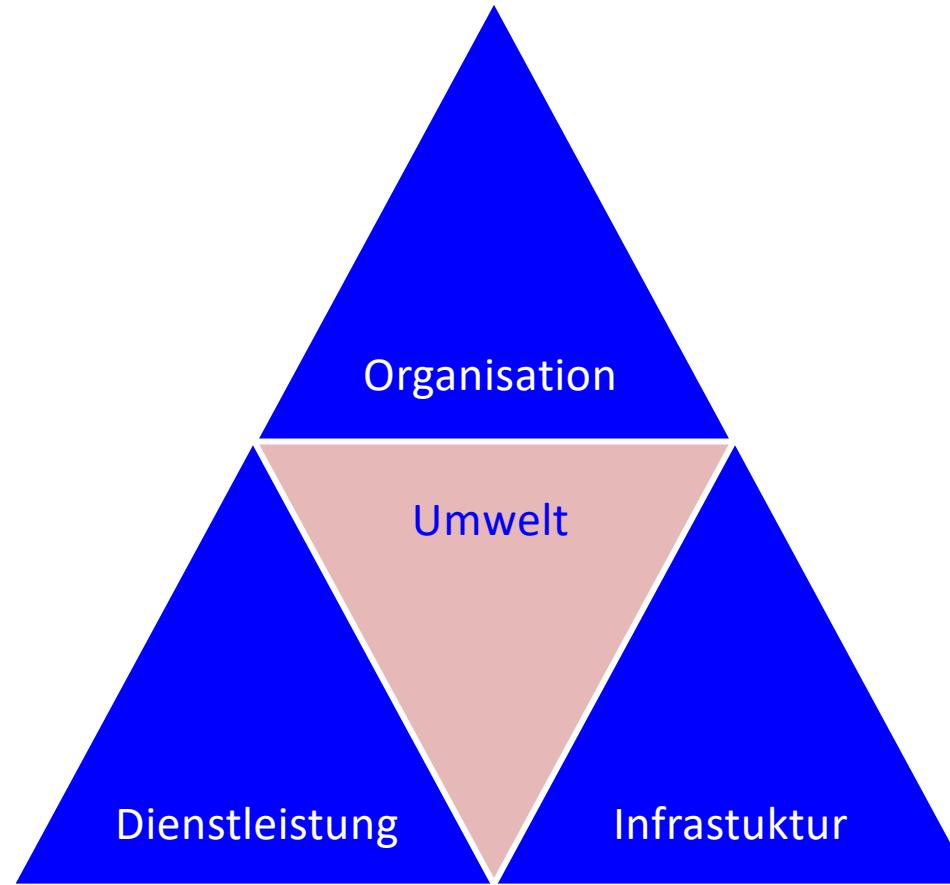
# Informationssicherheit die 8 kritischen Erfolgsfaktoren 1/2

1. Sicherheitspolitik, -ziele und -aktivitäten an den Geschäftszielen ausrichten
2. Implementierung in Übereinstimmung mit der Unternehmenskultur
3. Unterstützung durch das Management
4. eingehende Kenntnis der Sicherheitsanforderungen, Risikoanalyse und Risikomanagement

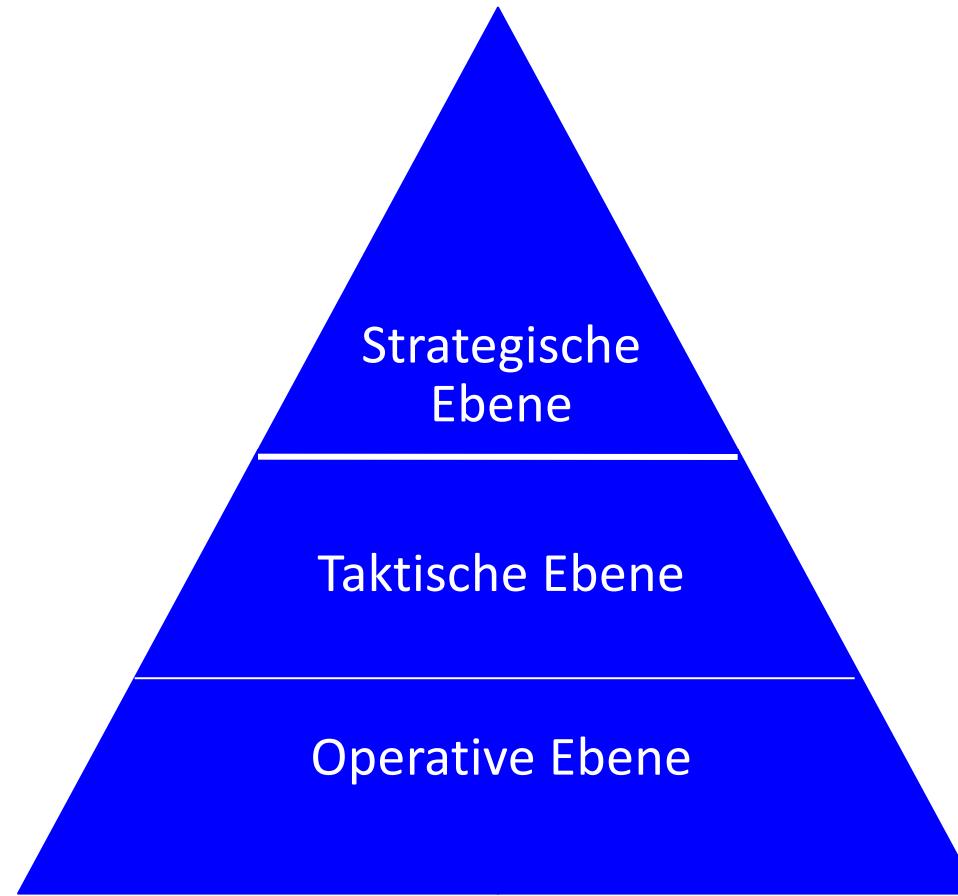
# Informationssicherheit die 8 kritischen Erfolgsfaktoren 1/2

5. Marketing von Sicherheit
6. Verteilung der Sicherheitsrichtlinie
7. Schulung
8. Prozess zur Bewertung und Verbesserung des Informationssicherheits Management Systems

# ISM-Framework 1/2



## ISM-Framework 2/2



# 4 Dimensionen ISM-Framework 1/4

- Umwelt
  - interne / externe Personen
  - gesetzliche Regulierungen / Restriktionen
  - ethische Aspekte
  - Organisationskultur
  - Verhalten der Mitarbeiter/innen
  - Interaktion mit anderen Organisationen, ...

# 4 Dimensionen ISM-Framework 2/4

- Organisation
  - Geschäftsprozesse
  - Verantwortlichkeiten
  - Steuerungswerzeuge
  - Betrachtung im Kontext des Informations- und Sicherheitsmanagements, ...

# 4 Dimensionen ISM-Framework 3/4

- Infrastruktur
  - Hardware
  - Software
  - Prozesse der Informationsverarbeitung
    - produktive Systeme
    - administrative Systeme
    - Systeme zur Wissensverarbeitung
  - Gebäude
  - Strom, ...

# 4 Dimensionen ISM-Framework 4/4

- Dienstleistung
  - alle Dienstleistungen
  - aber auch Produkte
  - an Dritte
  - wie auch Eigenleistungen

# Risikoträger

- unterschiedlich, je betrachteter Institution
- kann von einem Schaden betroffen sein
- muss das Risiko verantworten

# Was sind Informationen?

- Informationen sind **Geschäftswerte**
- von zentraler Bedeutung
- müssen aus unternehmerischer und rechtlicher Sicht **wirksam** geschützt werden
- Informationen werden in unterschiedlichen Formen übermittelt
- elektronisch ist **nur** eine Form

# Informationssicherheit

- muss umfassend betrachtet werden
- Risiken gibt es nicht nur in der Informationstechnologie
- Informationen müssen angemessen geschützt werden, unabhängig von
  - Form (Papier, Ton, Bild, ...)
  - Art der Nutzung
  - Art der Speicherung

# Zusammenfassung der Informationssicherheit

- Vertraulichkeit (confidentiality)
- Integrität (integrity)
- Verfügbarkeit (availability)
- Verbindlichkeit (accountability, non-repudiation)
- Authentizität (authenticity)
- Betriebssicherheit (reliability)

# Zusammenfassung der Informationssicherheit

- systematisch
- ganzheitlich
- kontinuierlich
- unternehmensspezifisch
- aktiv gelebt

# Zusammenfassung der Informationssicherheit

- Beurteilung der Risiken, damit die Informationswerte vor unberechtigter
  - Verwendung,
  - Veröffentlichung,
  - Veränderung,
  - Beschädigung und
  - Verlust geschützt werden

# Zusammenfassung der Informationssicherheit

Beurteilung der Risiken, damit angemessene Vorkehrungen getroffen werden,

- um die Wiederaufnahme der normalen Informationverarbeitung zu ermöglichen
- um weiterhin Informationsverarbeitung durchführen zu können

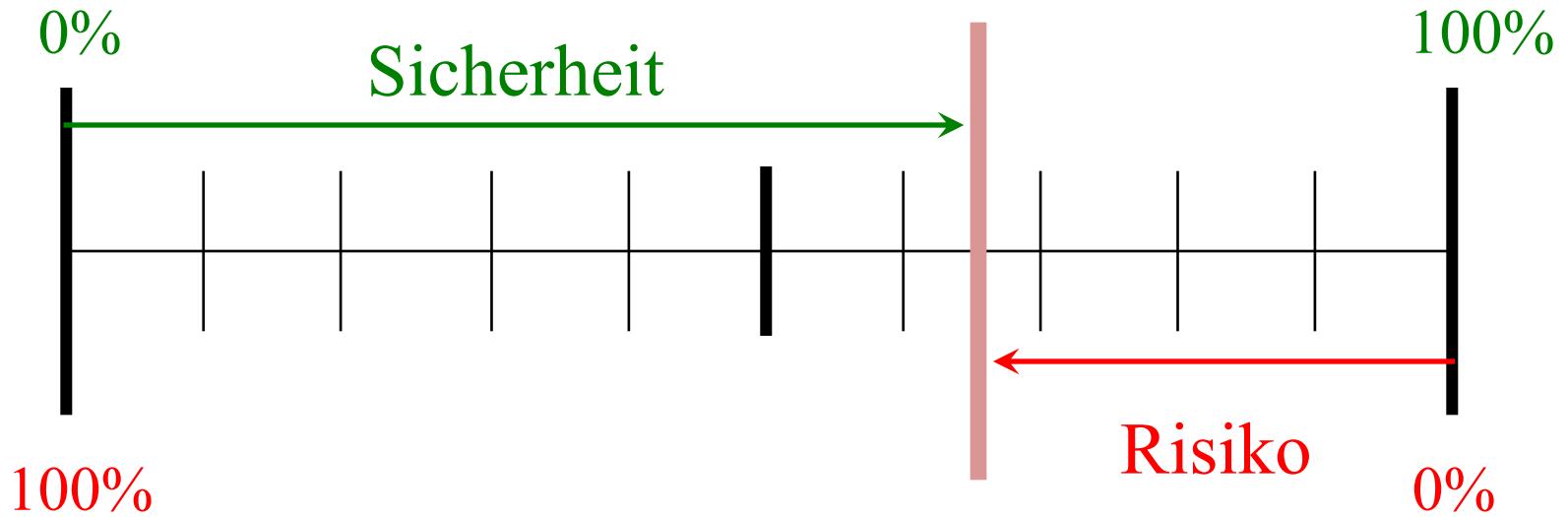
# Zusammenfassung der Informationssicherheit

- **Informationssicherheit** ist vorhanden durch
  - Vertraulichkeit
  - Verbindlichkeit
  - Integrität
  - Verfügbarkeit
- in einem **geplanten** Ausmass in den digitalen Prozessen auf IKT-Systemen

# I(K)T ist völlig unsicher

BIOS, Betriebssysteme, Programme,  
klassische materielle Komponenten, ...

# Sicherheit als Ziel



# Angriff aus den eigenen Reihen

Fahrlässigkeit, Sabotage, unberechtigte  
Kenntnisnahme, Hacker?, Cracker?, Phisher?, ...

# unkoordinierte Sicherheitsmaßnahmen

Zugangs-, Zugriffskontrolle, Identity Management,  
Verschlüsselung, Firewall, Virenschutz,  
Change & Patch Management, ...

# Ziele für das ELGA-ISMS

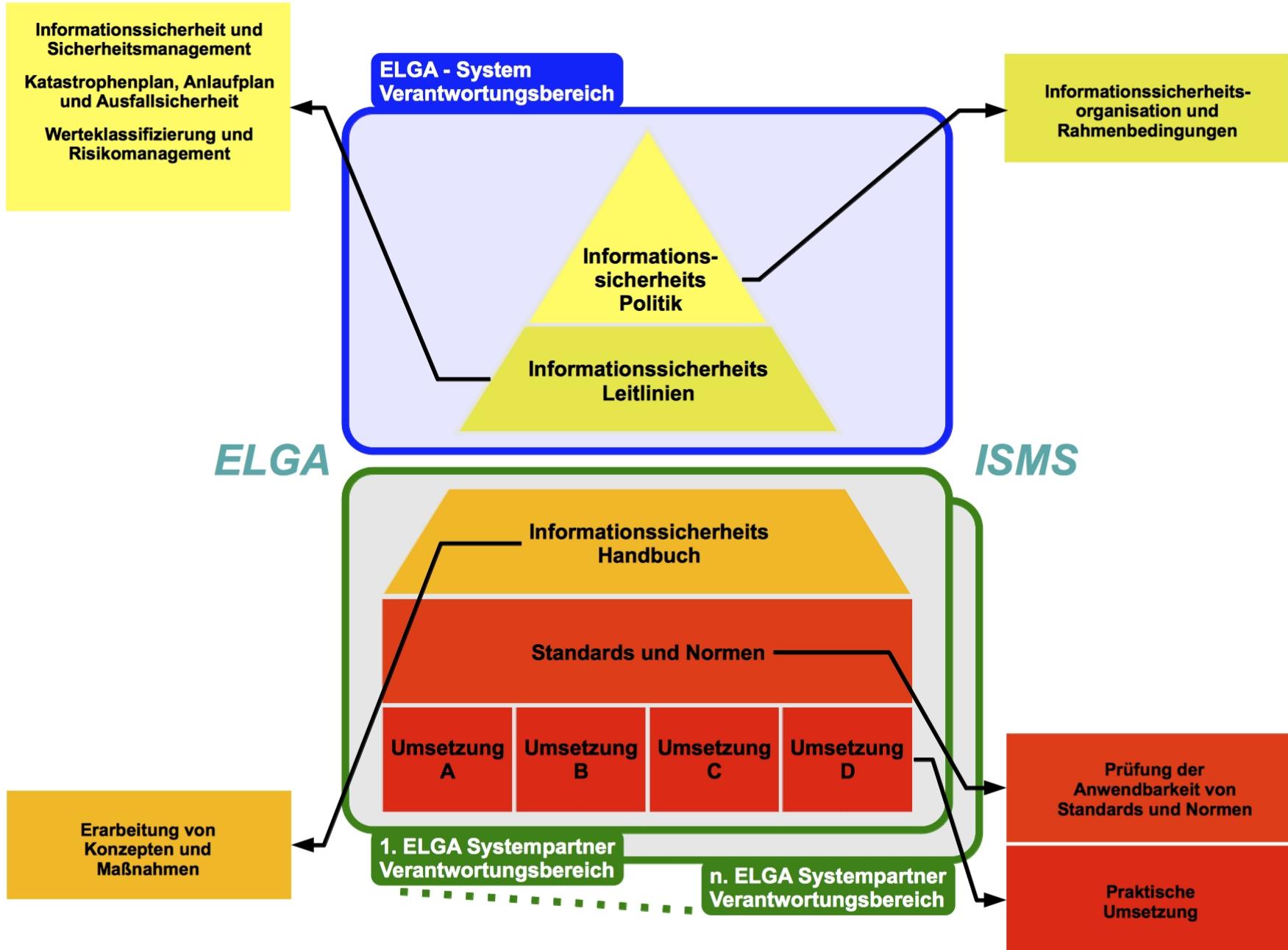
- Die **Verfügbarkeit** und Kontinuität des ELGA-Systems, unter Berücksichtigung der jeweiligen Rahmenbedingungen, ist bestmöglich erfüllt.
- die **Vertraulichkeit** und **Integrität** der im Zuge des ELGA-Systems erlangten Informationen und Daten ist sichergestellt.
- Die Einhaltung der rechtlichen Vorschriften unter Berücksichtigung der **gesamtheitlichen Betrachtung** im ELGA-System ist gewährleistet.
- Das mit den ELGA-Systempartnern **abgestimmtes Informationssicherheitskonzept** ist im ELGA-System umgesetzt.

# Verantwortung im ELGA-System 1/2

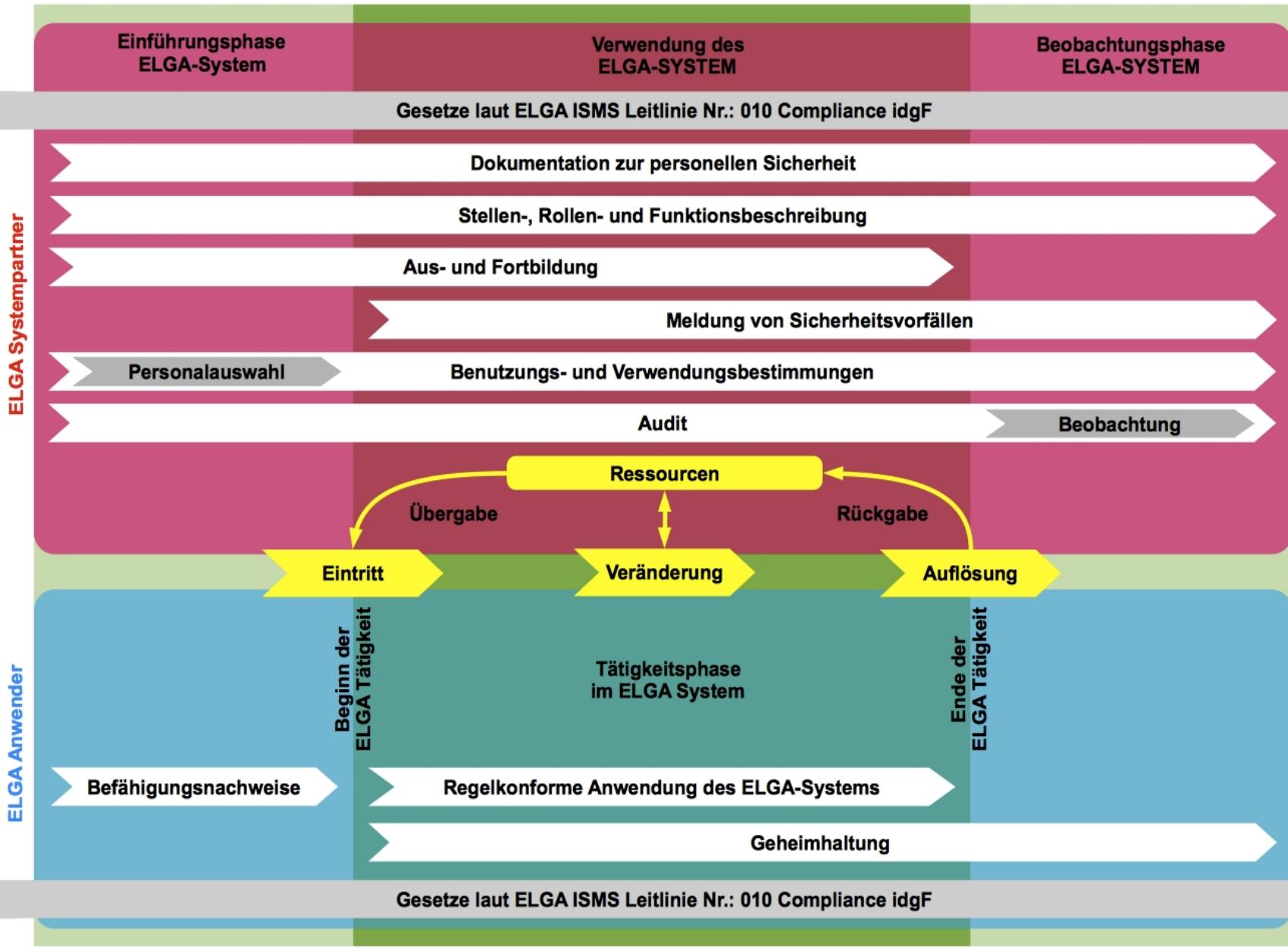
- Die ELGA-Systempartner sind sich der Problematik und **Verantwortung bewusst** und haben aus diesem Grund die Einführung des ELGA-ISMS beschlossen.
- Im Rahmen des ELGA-ISMS wird von allen beteiligten ELGA-Systempartnern und deren Mitarbeitern erwartet, dass sie sich entsprechend dieser Politik und den daraus abgeleiteten Vorgaben und **ELGA-ISMS Leitlinien** verhalten, sich der eigenen Verantwortung bewusst sind und eine **hohe Sensibilität** für Informationssicherheit im ELGA-System aufweisen.
- Es wird vorausgesetzt, dass die gemeinsam etablierte ELGA-ISMS Organisation und die mit der Ausführung beauftragten Verantwortlichen sowie andere Beauftragte bei der Ausübung ihrer Tätigkeit durch das **Management** der jeweiligen ELGA-Systempartner **aktiv unterstützt** werden.

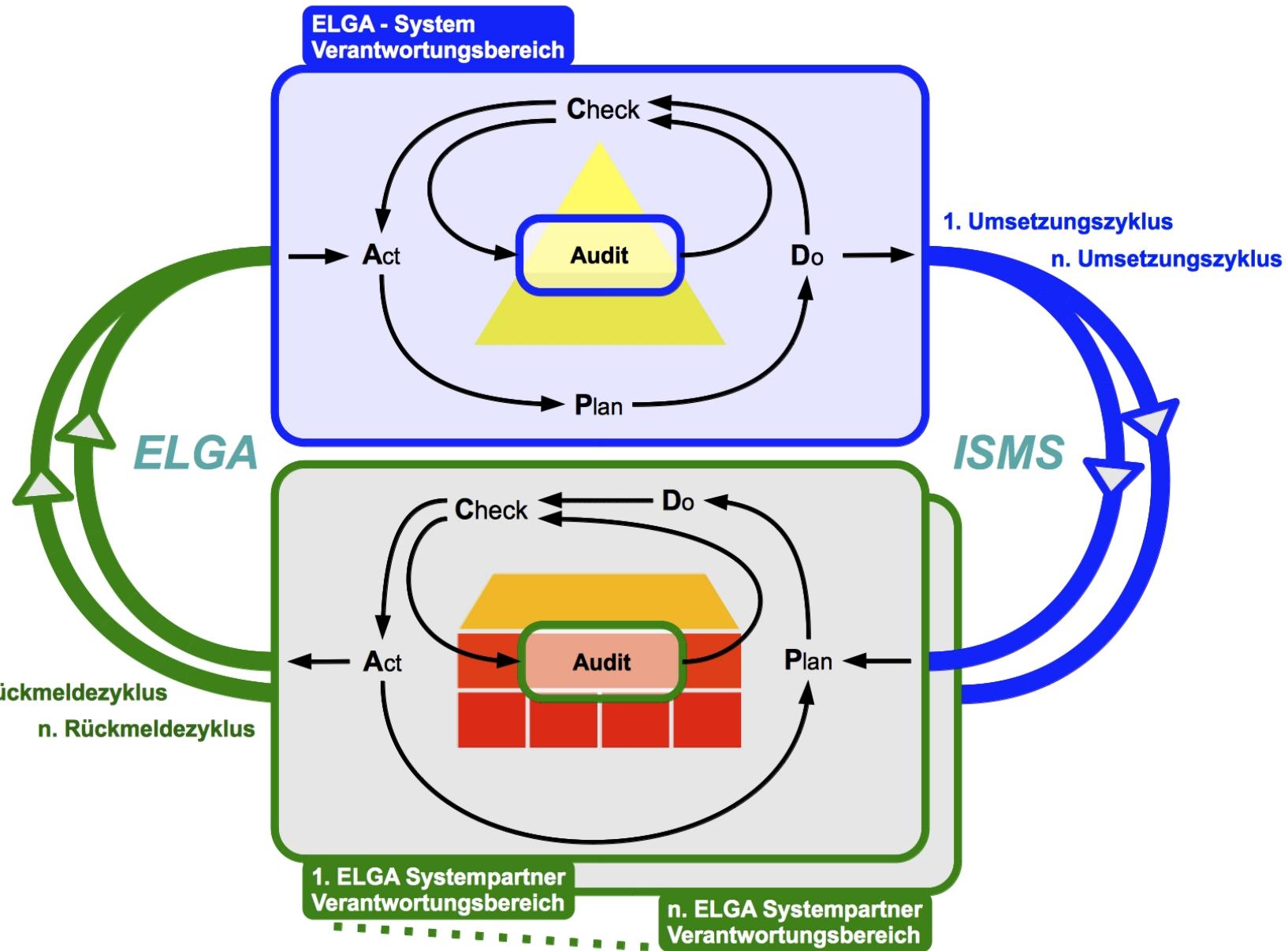
# Verantwortung im ELGA-System 2/2

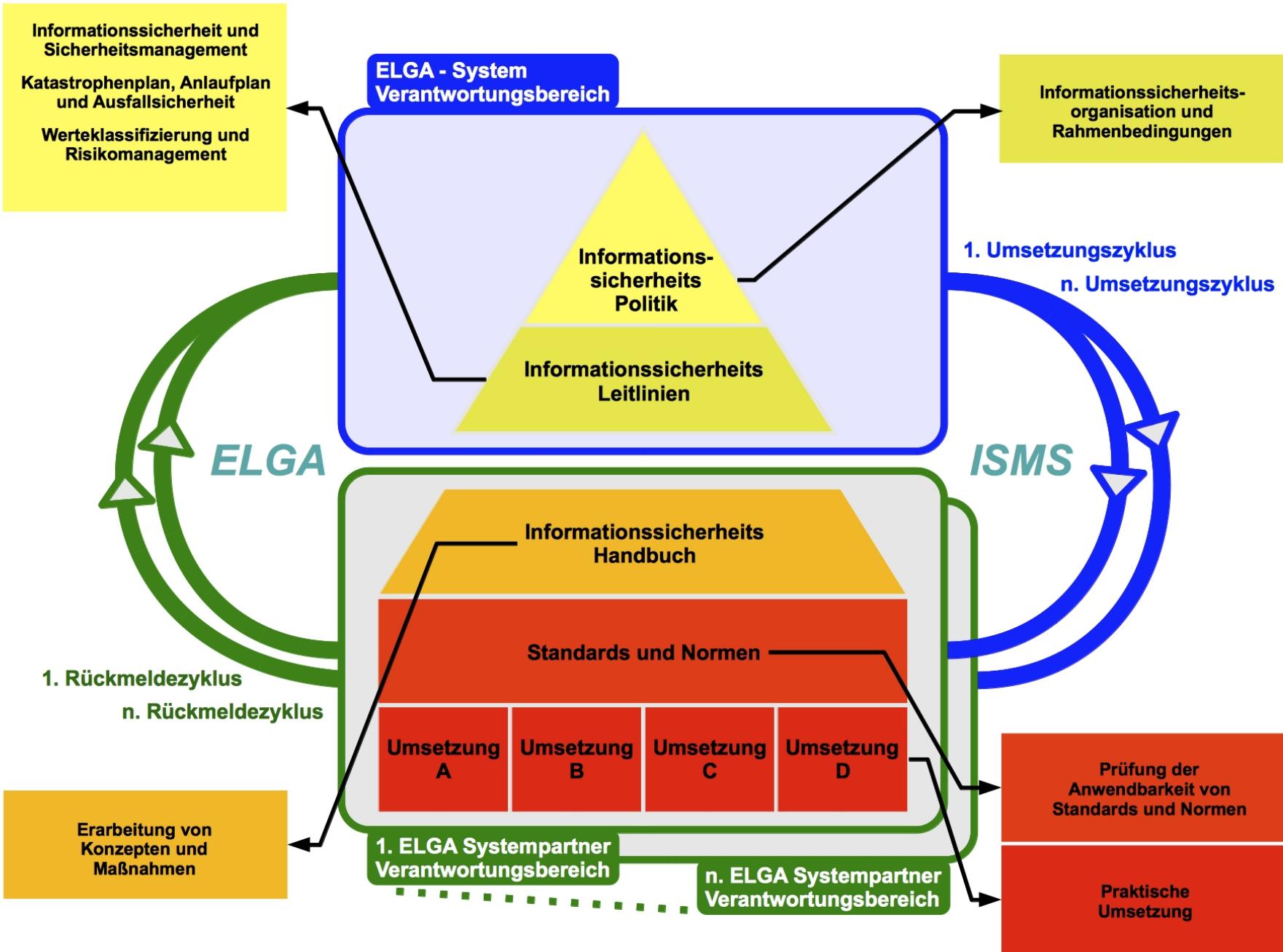
- Die ELGA-ISMS Organisation ist entsprechend der ELGA-ISMS Leitlinien auch mit den **erforderlichen Kompetenzen ausgestattet**.
- Die Informationssicherheitspolitik und die daraus abgeleiteten **ELGA-ISMS Leitlinien sind** bei allen beteiligten ELGA-Systempartnern **verbindlich** und müssen allen Mitarbeitern, die mit dem ELGA-System befasst sind, nachweisbar zur Kenntnis gebracht werden.
- Die Informationssicherheitspolitik bezieht sich auf **sämtliche Tätigkeiten, Funktionen und Prozesse**, die zur Erreichung der Ziele des ELGA-Systems ausgeführt werden, wobei sowohl auf Gefahrenpotentiale von Innen (sei es durch den Betrieb technisch sensibler Geräte oder auch durch die Mitarbeiter) als auch auf Bedrohungen von Außen Bedacht zu nehmen ist



# Prozesslandschaft der personellen ELGA Sicherheit des ELGA System



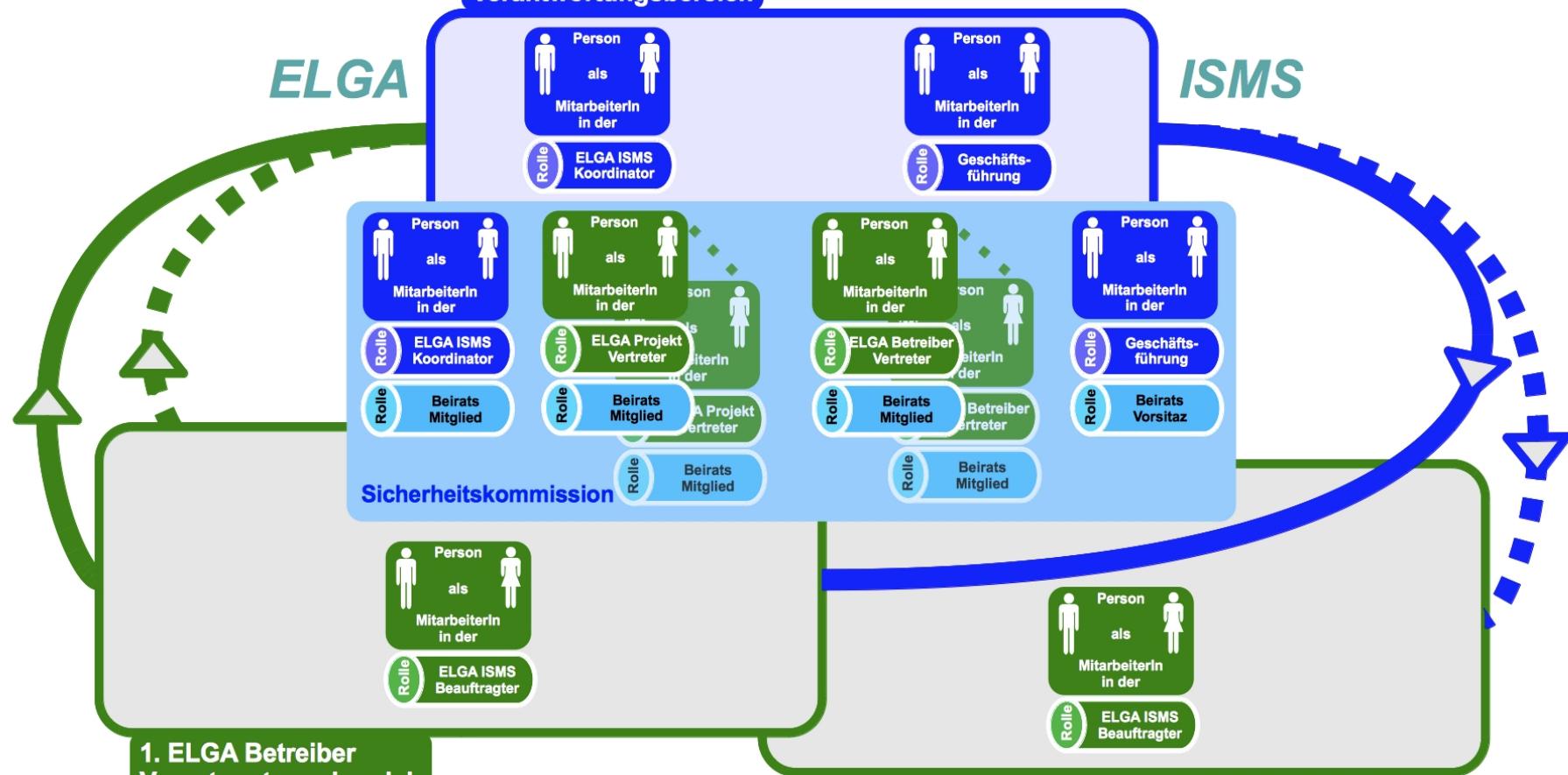




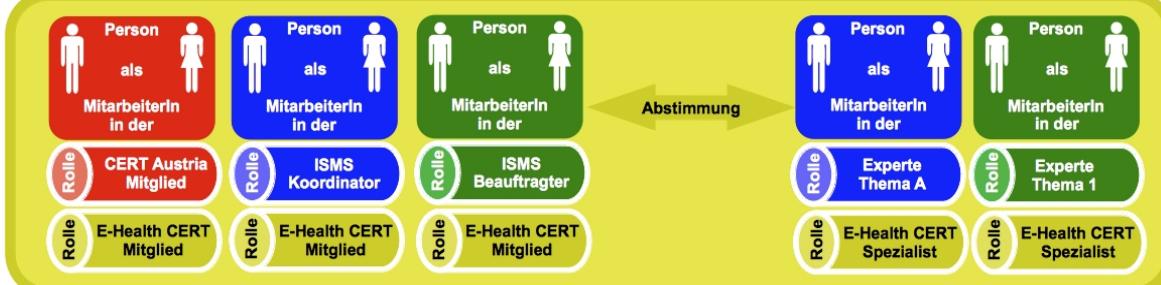
## ELGA Verantwortungsbereich

**ELGA**

**ISMS**

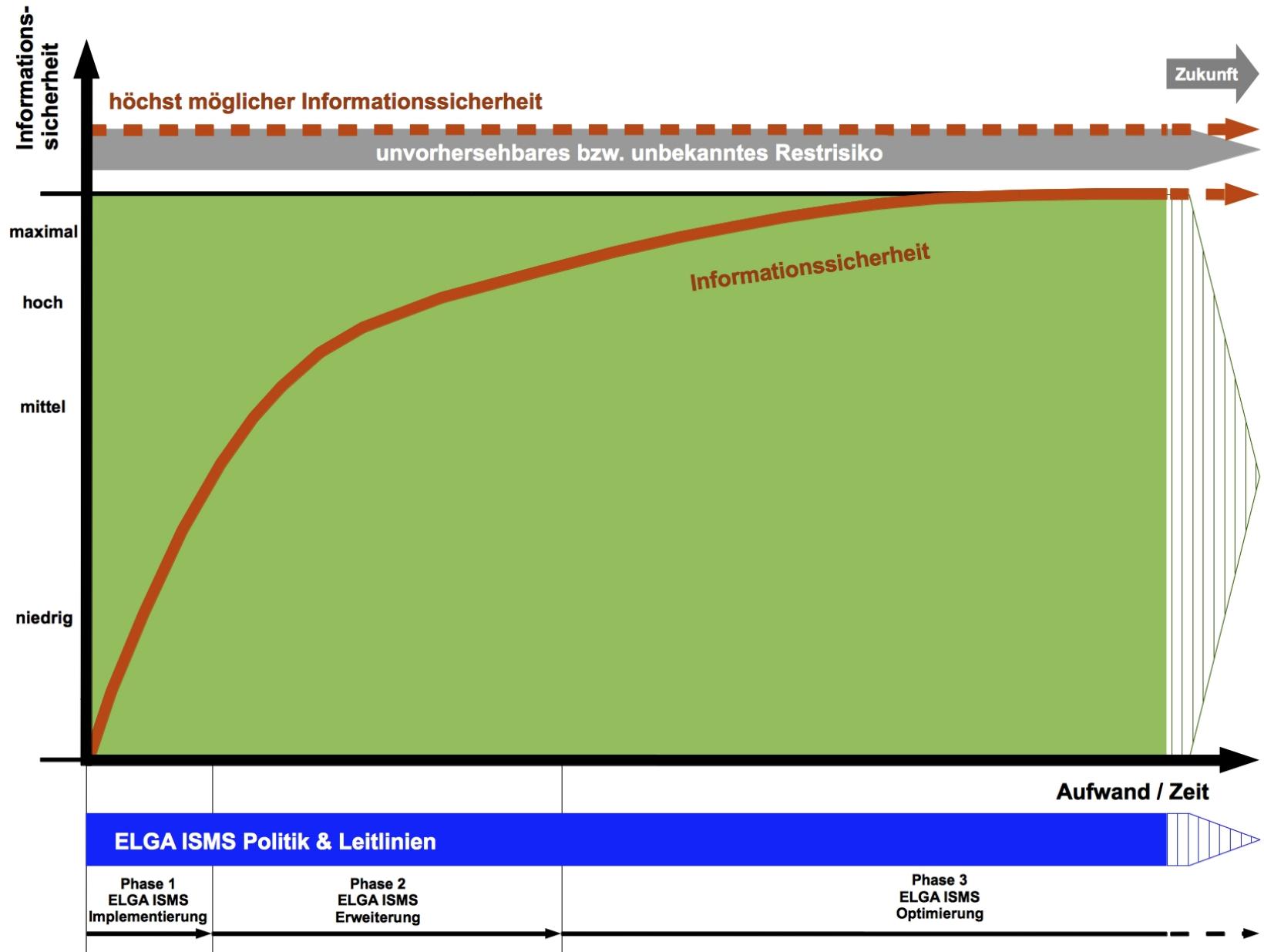


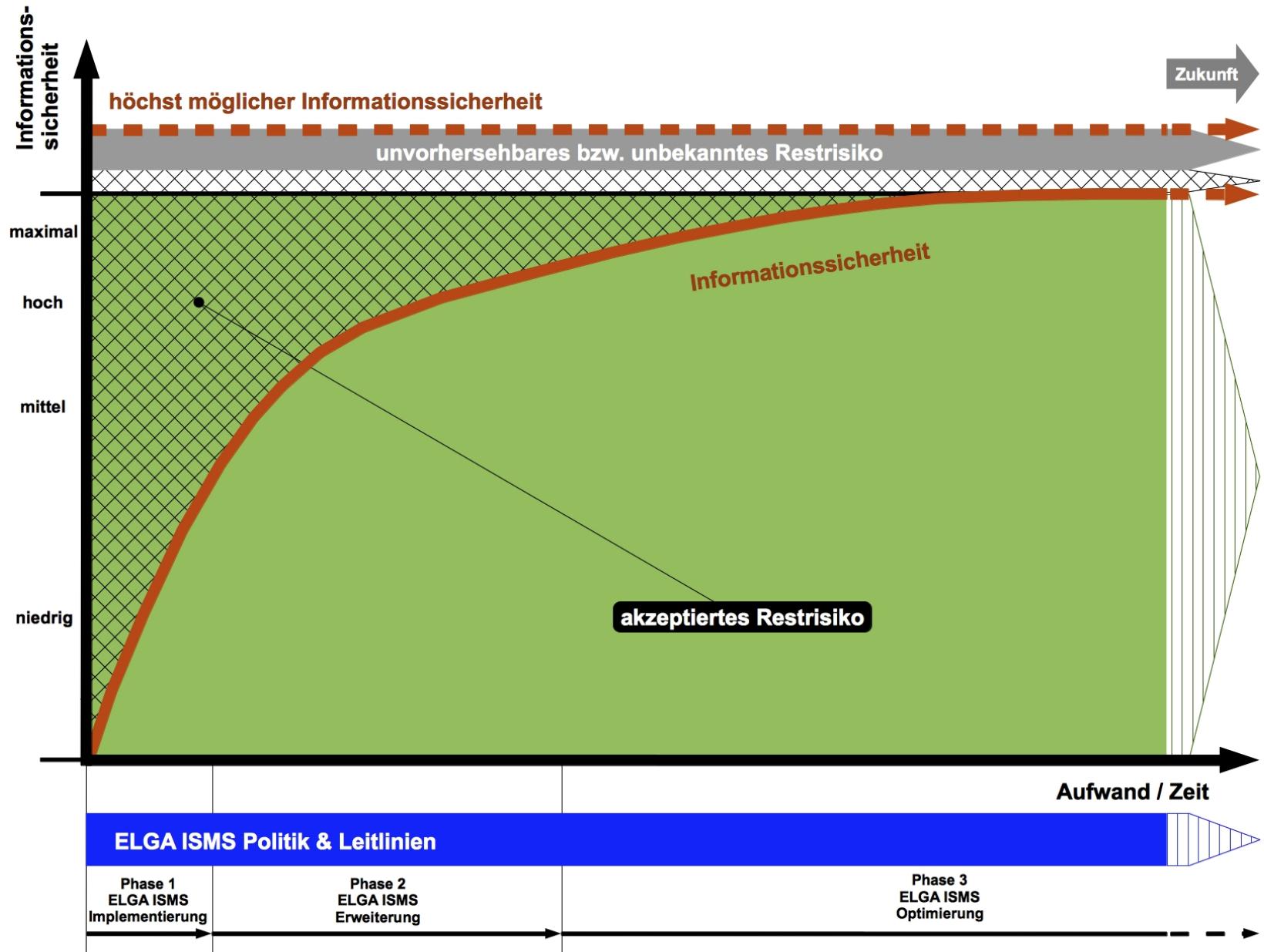
## E-Health CERT

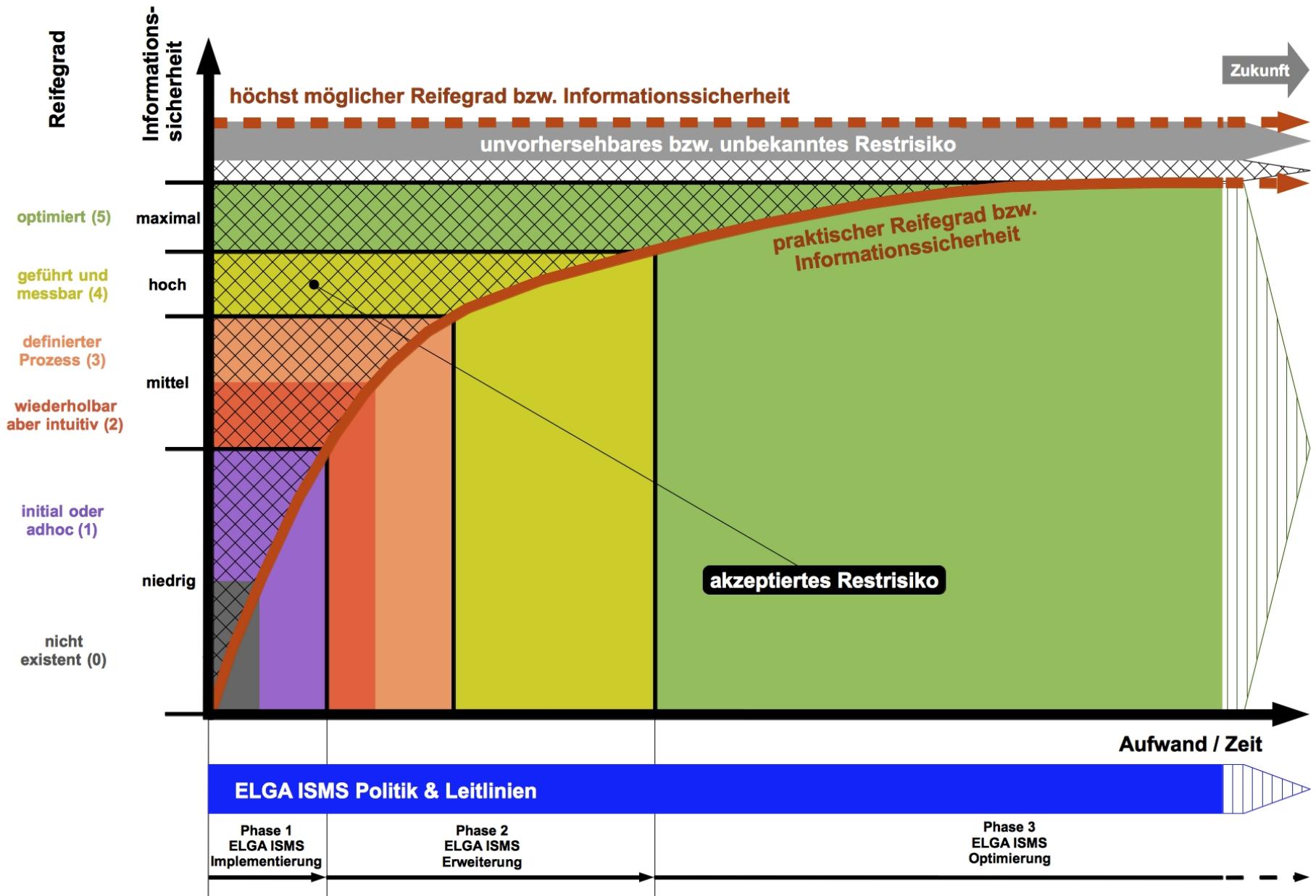


# Grundsätze

- Durch ELGA-ISMS mit den darauf basierenden nachgelagerten Leitlinien und ggf. daraus abgeleiteten Checklisten und Empfehlungen wird / werden
  - ein **hohes Sicherheitsbewusstsein** geschaffen,
  - der Aufbau einer **übergreifenden Informationssicherheitsorganisation** (ISiOrg - Struktur und Ablauf) festgelegt,
  - die jeweiligen Aufgaben und Verantwortlichkeiten mit den erforderlichen **Kompetenzen zugewiesen**,
  - die **Basis für eine kontinuierliche Weiterentwicklung** der Informationssicherheitsprozesse geschaffen,
  - und gemeinsame Mindeststandards von Informationssicherheitsmaßnahmen nach **einheitlichen Grundsätzen** festgelegt







## was fehlt oft noch

- standardisiertes Risikomanagement MT/IKT-Technik
- klare Abstimmung der Nahtstellen & Verantwortlichkeiten
- gemeinsame GRC-Anforderungen
- Transparente Informationen über die Auswirkung von IKT-Ausfällen auf den medizinische Behandlungsprozess
- Betreiber kennt das Risiko und entscheidet bewusst über die Akzeptanz von Restrisiken
- Herstellerinformationen über ihre Risikobewertung
- Change-, Patch- und Versionsmanagement
- Anwender ist sich bewusst, dass jedes technische System ausfallen kann und kennt die NOTFALLPLÄNE

# Warum brauchen wir Datenschutz & Informationssicherheit

- Unser Gesundheitssystem ist arbeitsteilig, sektoral und „mangelhaft“ vernetzt und soll sich in der Zukunft immer mehr vernetzen
- es hat die gleichen Verwundbarkeiten und muss lernen mit SECURITY umzugehen, auch wenn es SAFETY bereits anwenden kann
- Anpassungsbedarf
  - neue Technologien brauchen neue Organisationsformen
  - Integration und Kooperationen über Organisationsgrenzen
  - Vertrauen hat viele Gesichter, einige sollte ich kennen