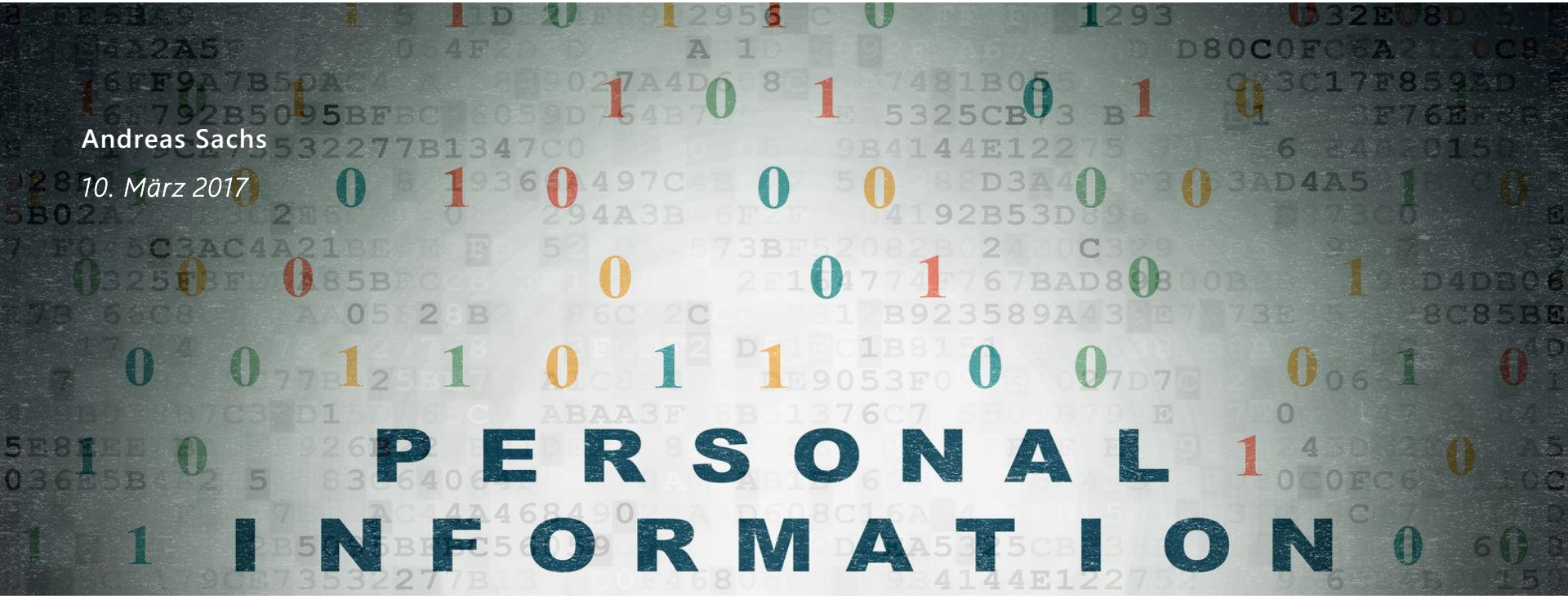
Andreas Sachs

10. März 2017



Vorgaben zur IT-Sicherheit in der DS-GVO

Kurzvorstellung des Referenten

Andreas Sachs

ist Informatiker und Stellvertretender Leiter des *Bayerischen Landesamts für Datenschutzaufsicht* in Ansbach.

Seit 2011 beschäftigt sich das technische Referat mit verschiedensten Themenfelder, u. a.:


Internet der Dinge


Verschlüsselungsverfahren


Datenpannen & Hacking


Vernetzte Fahrzeuge


Cloud Computing


IT-Sicherheit


Identitäten & Webportale


Apps & Smart Devices


Trackingverfahren

I Den Fokus finden

Verhältnis von IT-Sicherheit zum Datenschutz

Datenschutz:
Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten
(Blick auf das Persönlichkeitsrecht)

↓

Umfasst rechtliche,
technische und organisatorische Regelungen

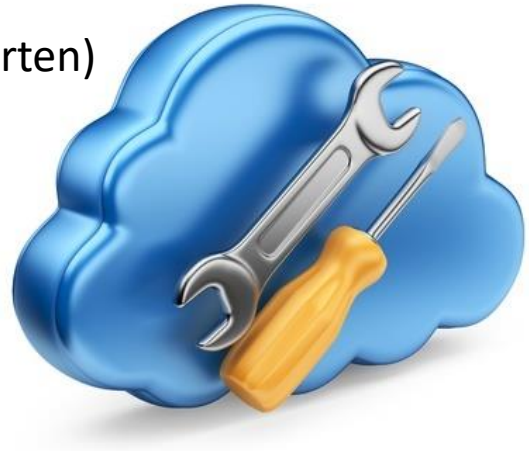
IT-Sicherheit hat „normalerweise“ die **Unternehmenswerte** im Blick:
- Aber: Schutz personenbezogener Daten ist auch ein Unternehmenswert (z.B. Kundenverlust, Gefahr von Sanktionen, Verstoß gegen Compliance,…)
- Unternehmen sind grundsätzlich frei, gewisse Restrisiken zu akzeptieren. Dies ist bei personenbezogenen Daten nicht möglich (gesetzliche Regelungen)

Fazit: Methoden der IT-Sicherheit müssen den **einzelnen Betroffenen** in den **Blickwinkel** nehmen

I Den Fokus finden

Verhältnis von IT-Sicherheit zum Datenschutz

Technischer Datenschutz:
Umfasst **Methoden** der (auf personenbezogenen Daten fokussierten) **IT-Sicherheit** sowie **weitere Blickwinkel**, die in der IT-Sicherheit eher keine bzw. manchmal eine gegensätzliche Rolle spielen



Beispiele (aus DS-GVO):
Umsetzung des Grundsatzes der **Datenminimierung**
Sicherstellung der **Zweckbindung**
Transparente Datenverarbeitung
Löschung/“Sperrung“/Berichtigung von Daten
Anonymisierung/Pseudonymisierung

I Den Fokus finden

IT-Sicherheit und personenbezogene Daten

IT-Sicherheit
Informationssicherheit
„Cybersicherheit“

Unterteilung

Security (Schutz vor vorsätzlichem Handeln)
Safety (Schutz vor fahrlässigem Handeln / höherer Gewalt)

Schutz der Vertraulichkeit,
Verfügbarkeit und Integrität
(personenbezogener) Daten

Betrachtung von:
Daten, IT-Systemen, Prozessen und Menschen

II Datenschutzgrundverordnung

§ 9 BDSG (samt Anlage)

Maßnahmen- bzw. Kontrollzentrierter Ansatz

Die DS-GVO sollte nicht mit dem Blickwinkel, *es hat sich doch gar nicht so viel geändert,* angesehen werden („Trennungsschmerz“ ☹)

II Datenschutzgrundverordnung

§ 9 BDSG (samt Anlage)

Probleme des § 9 BDSG (samt Anlage)

- § 9 BDSG ist sehr Allgemein
- Anlage zu § 9 BDSG wird häufig als Checkliste abgearbeitet
- Sind die technischen und organisatorischen Maßnahmen(TOMs) vollständig?
- Sind die technischen und organisatorischen Maßnahmen wirksam?
- Sind Prozesse bei den verantwortlichen Stellen vorhanden?
- Welche Maßstäbe gelten bei der Auswahl der TOMs?
- Bei welchen Verarbeitungen werden diese eingesetzt?
- Sind (Datenschutz-)Managementsysteme bislang verpflichtend?

II Datenschutzgrundverordnung

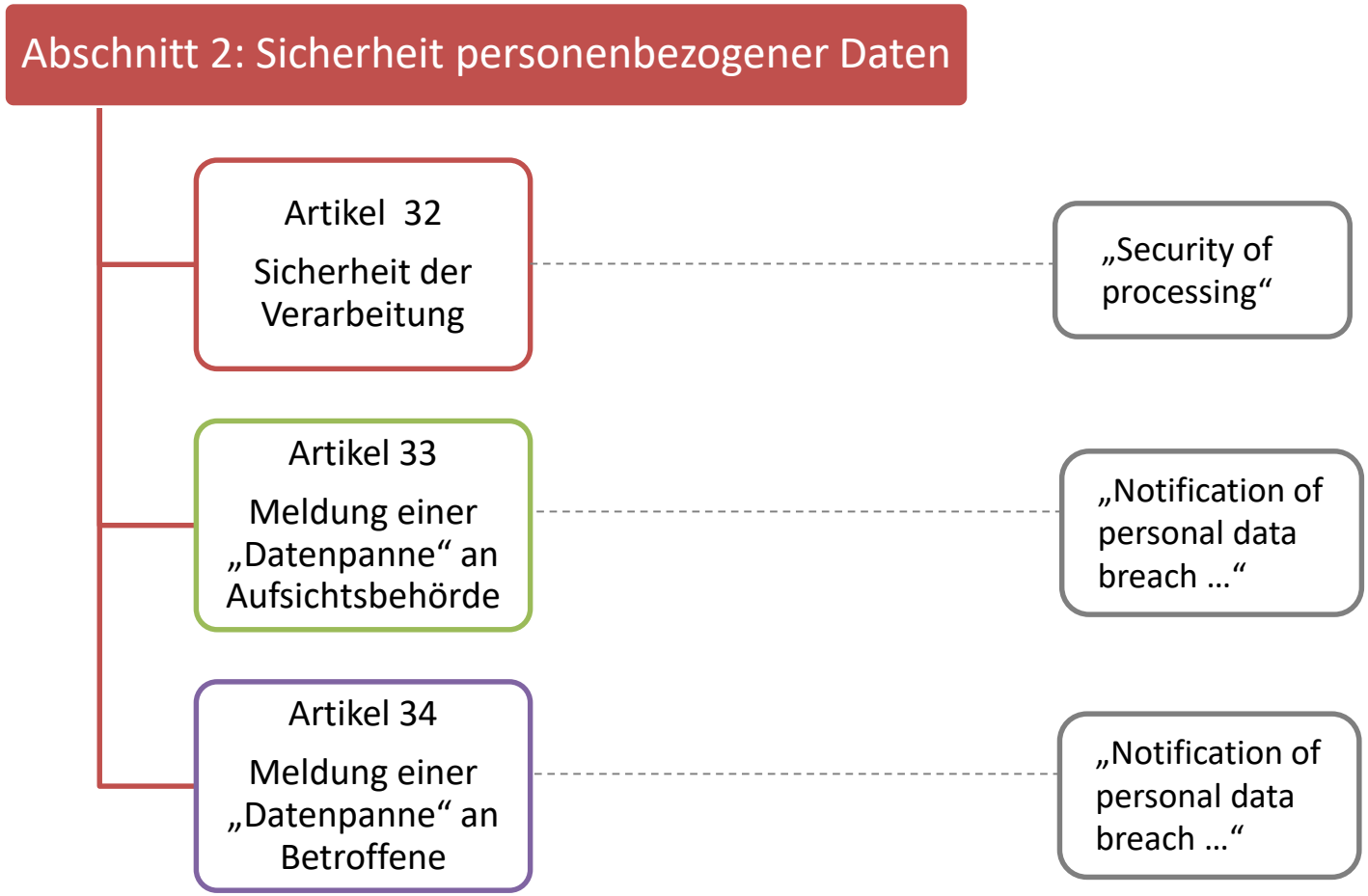
„Technik“ in der DS-GVO

Bei welchen Bereichen kommen **technische und organisatorische Maßnahmen** in der DS-GVO vor?

Transparenz	Datenminimierung	Betroffenenrechte	Löschung/Sperrung
Datenschutzkonforme Verarbeitung	Security	Profiling	Rechenschaftspflicht
Managementsysteme	ADV	„Big-Data“	Zweckbindung
Speicherbegrenzung	Privacy by Design/Default	Datenschutzfolge-abschätzung	Weiteres?

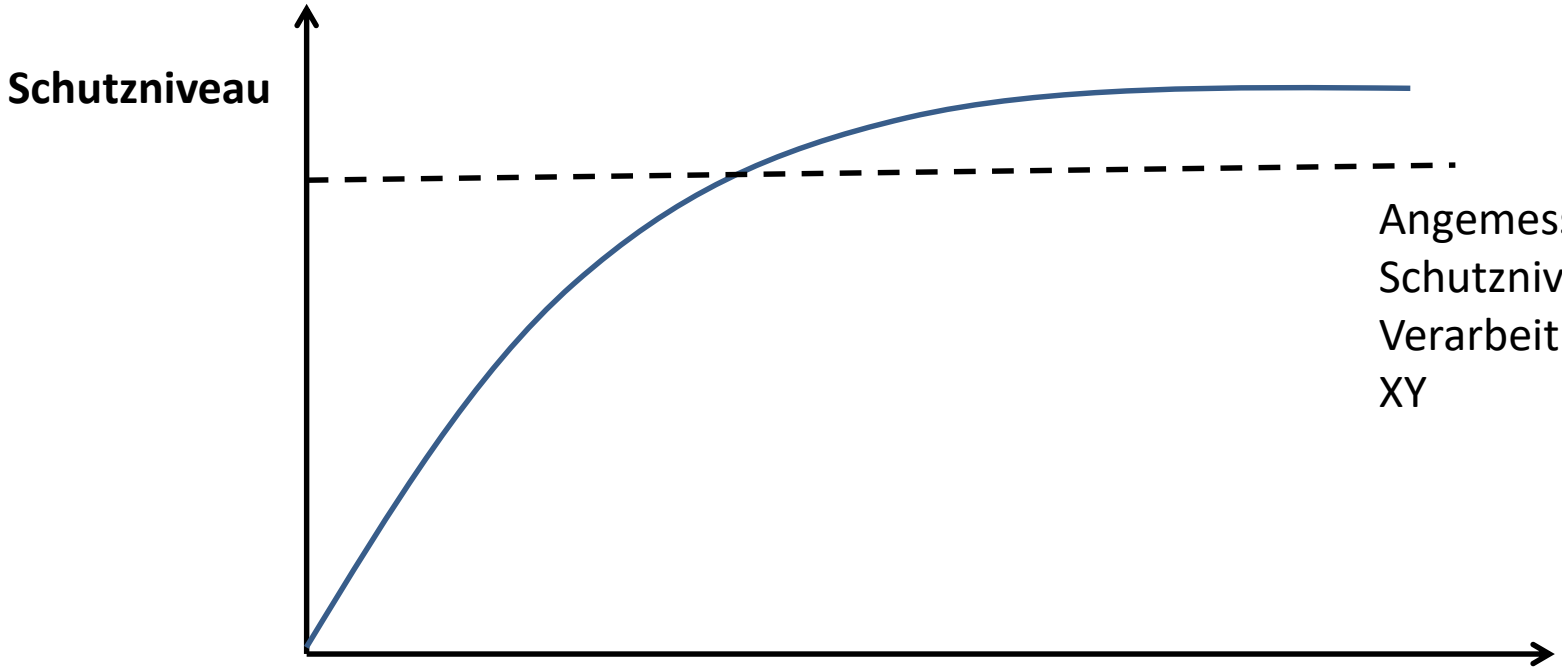
III Sicherheit personenbezogener Daten

Überblick



III Sicherheit der Verarbeitung

Angemessenes Schutzniveau

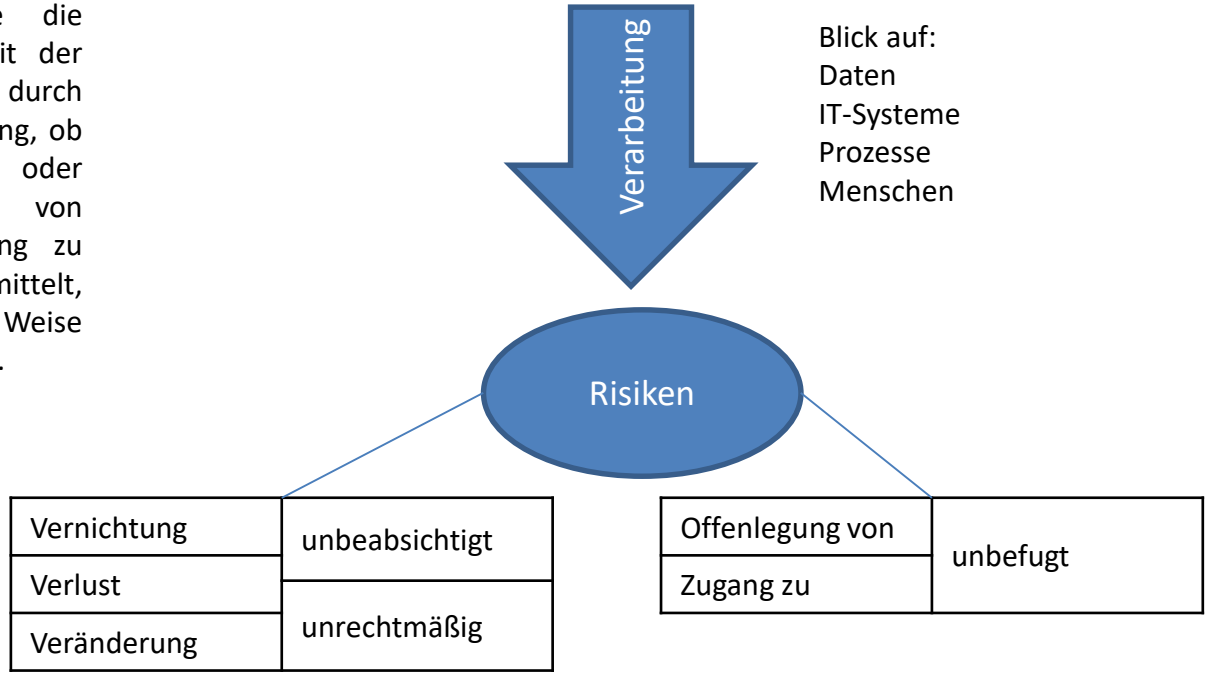


III Sicherheit der Verarbeitung

Angemessenes Schutzniveau

Artikel 32 Abs. 2 DS-GVO
Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Personenbezogene Daten



„Klassische“ Schutzziele der IT-Sicherheit

Verlust der **Verfügbarkeit** und **Integrität** der Daten

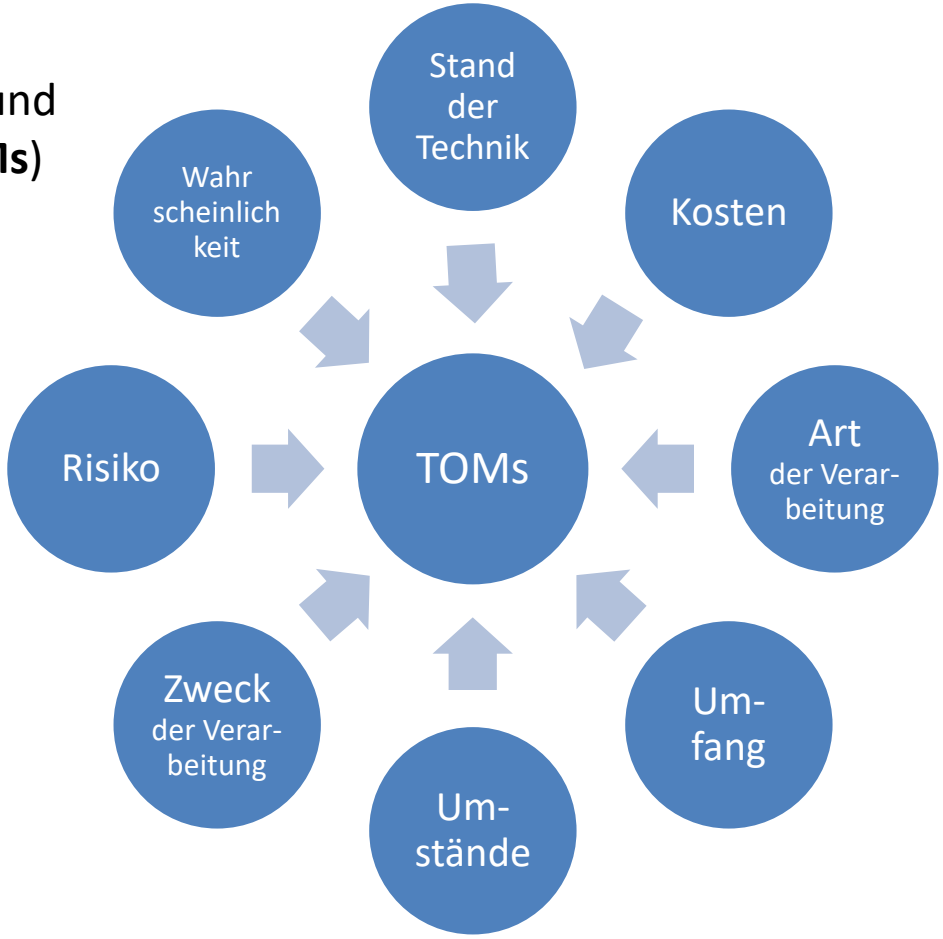
Verlust der **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** der Daten

III Sicherheit personenbezogener Daten

Faktoren zur Auswahl von TOMs

Es müssen (wie bisher) technische und organisatorische Maßnahmen (**TOMs**) getroffen werden
(Artikel 32, Absatz 1 DS-GVO)

Neu:
Explizite Nennung der Faktoren, die dabei eine Rolle spielen



III Sicherheit personenbezogener Daten

Artikel 32: TOM „Pseudonymisierung“

Explizite Nennung von Pseudonymisierung

Was versteht man darunter?
„Pseudonyme können durch Heranziehen weiterer Informationen einer natürlichen Person zugeordnet werden (EW 26)“

Intention der Pseudonymisierung:
*„Die Anwendung der **Pseudonymisierung** auf personenbezogene Daten **kann die Risiken** für die betroffenen Personen **senken** (EW 28)“*

Beispiele:
- Trennung von Patientendaten und medizinischen Daten
- Pseudonymisierung vor zulässiger statistischer Auswertung

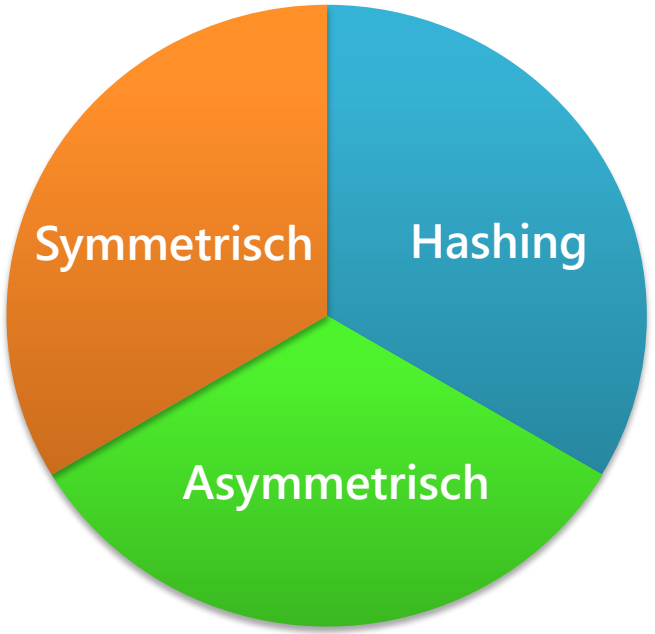
III Sicherheit personenbezogener Daten

Artikel 32: Sicherheit der Verarbeitung

Explizite Nennung von Verschlüsselung

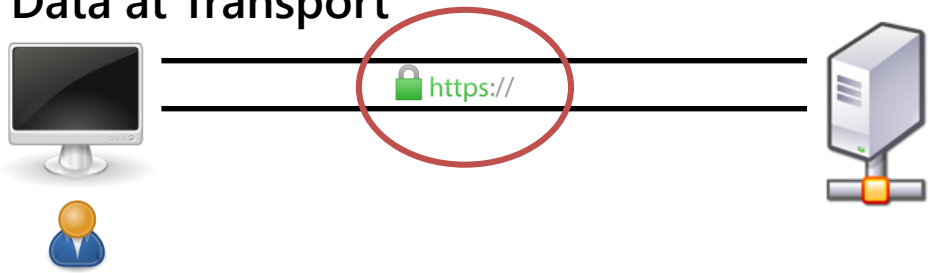
Berücksichtigung des **Standes der Technik**

Drei grundlegende Erscheinungen im (Datenschutz-)Alltag

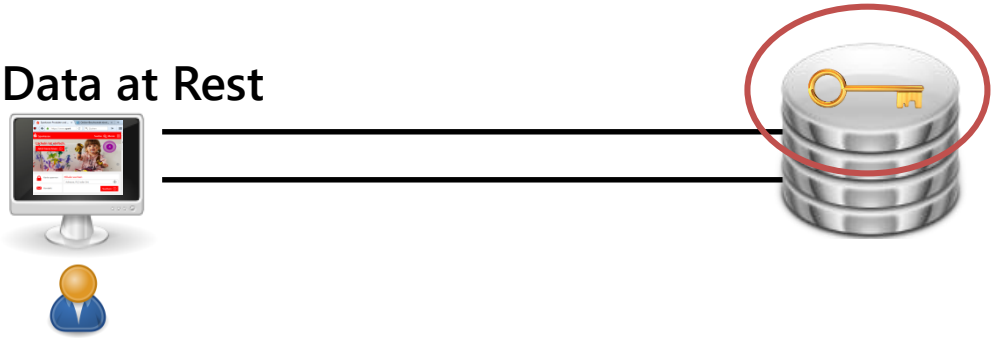


Verschlüsselung: Drei verschiedene Prinzipien

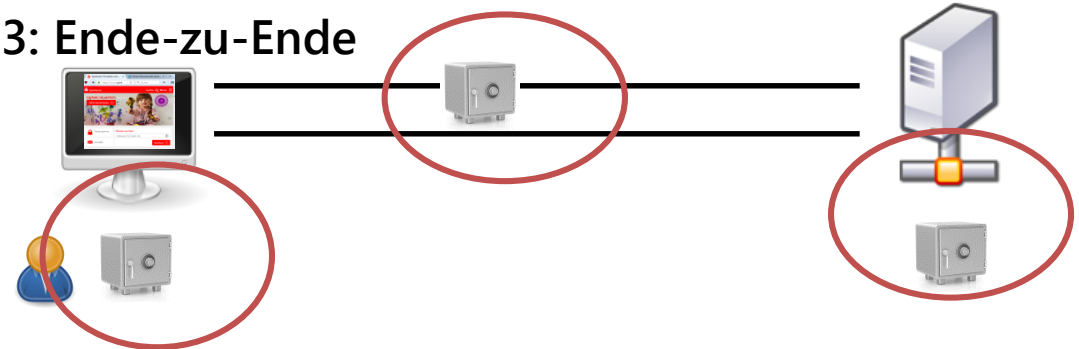
1: Data at Transport



2: Data at Rest



3: Ende-zu-Ende

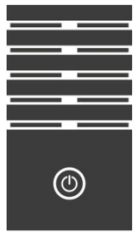


III Sicherheit personenbezogener Daten

Artikel 32: Sicherheit der Verarbeitung

Explizite Nennung von: Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit

- Vertraulichkeit
- Verfügbarkeit
- Integrität
- Belastbarkeit



Die Klassiker in der **Informationssicherheit**
(bis auf Belastbarkeit)

die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der **Systeme und Dienste** im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; (Art. 32, Abs. 1, Lit. b)

III Sicherheit personenbezogener Daten

Artikel 32: Sicherheit der Verarbeitung

Explizite Nennung von:
Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen **Zwischenfall** rasch wiederherzustellen;

⇨ Safety

Umsetzung:
- ⇨ Backup-Konzept
- ⇨ Redundante Datenspeicherung
- ⇨ Cloud Services
- ⇨ Anonymisierung durch Verschlüsselung (noch möglich?)

III Sicherheit personenbezogener Daten

Artikel 32: Sicherheit der Verarbeitung

Explizite Nennung von:
ein **Verfahren** zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

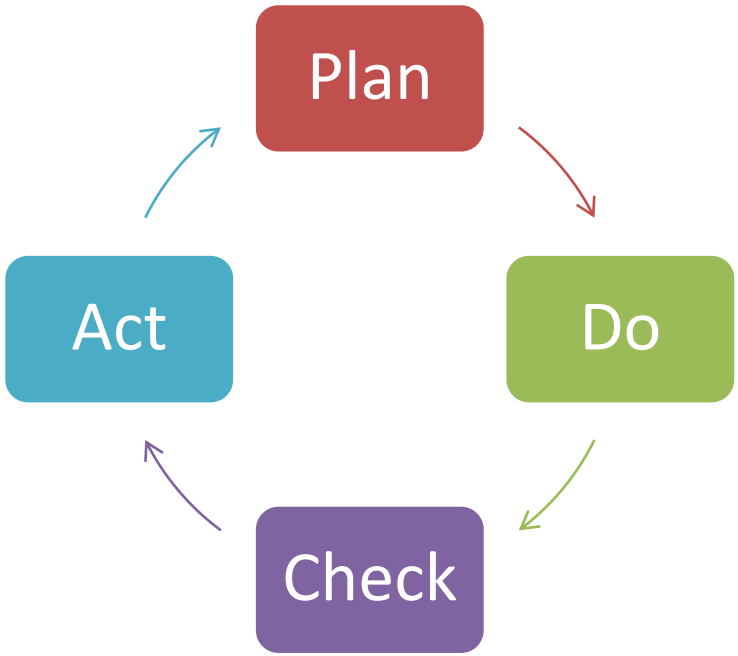
➡ Prozessorientierter Ansatz:

Plan:
Entwicklung eines Sicherheits-/Datenschutzkonzepts

Do:
Risikobewertung und Einführung von TOMs

Check:
Überwachung der Wirksamkeit/Vollständigkeit

Act:
Kontinuierliche Verbesserung



III Sicherheit personenbezogener Daten

Risiko

Der Begriff „Risiko“ kommt 32 mal in der Grundverordnung vor
Der Begriff „hohes Risiko“ 14 mal

Was wird denn darunter in der DS-GVO genau verstanden?

<u>Objektiv (ErwGr. 76)</u>
*Das Risiko sollte anhand einer **objektiven Bewertung** beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.*

<u>Berechnungsmethode (ErwGr. 76)</u>
Eintrittswahrscheinlichkeit und **Schwere** des Risikos für die **Rechte und Freiheiten** der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden.

Risiko – Rechte und Freiheiten

Das Risiko bezieht sich auf die **Rechte und Freiheiten** natürlicher Personen bei der Verarbeitung personenbezogener Daten.

Was versteht die DS-GVO unter den „Rechten und Freiheiten“ im Kontext Risiko und Schutz?

Ein Risiko ist immer ein mögliches, auf die **Zukunft** gerichtetes Ereignis.
Tritt dieses ein, dann kommt es ggf. zu einem **Schaden**

<u>Blick auf ErwGr. 75:</u>
Risiken für die Rechte und Freiheiten natürlicher Personen … können zu einem
physischen
materiellen
immateriellen
Schaden führen.

III Sicherheit personenbezogener Daten

Risiko – Rechte und Freiheiten

Beispiele für Risiken der Rechte und Freiheiten (ErwGr. 75)

Diskriminierung
Bsp: Teurere Kredite für bestimmte Bewohner bestimmter Stadtviertel

Identitätsdiebstahl
Bsp: Hacking eines Online-Shops und Verkauf der Daten im Darknet

Finanzieller Verlust
Bsp: Banking-Trojaner auf Smartphone und PC

Rufschädigung
Bsp: Big-Data-Analyst erzählt im Sportverein die Zielgruppenbestimmung des Nachbarn

Verlust der Vertraulichkeit von Daten, die dem Berufsgeheimnis unterliegen
Bsp: Fehlversand einer Privatrechnung durch einen Psychiater

Risiko – Rechte und Freiheiten

Beispiele für Risiken der Rechte und Freiheiten (ErwGr. 75)

Unbefugte Aufhebung der Pseudonymisierung

Bsp: Offenbarung von Name und Adresse zu einem Pseudonym eines sozialen Netzwerkes durch einen Programmierfehler

Hinderung der Kontrolle über die eigenen Daten

Bsp: Keine Möglichkeit, gepostete Fotos auf einem Dating-Portal zu löschen

Verarbeitung von sensiblen Daten (nach Artikel 9 DS-GVO)

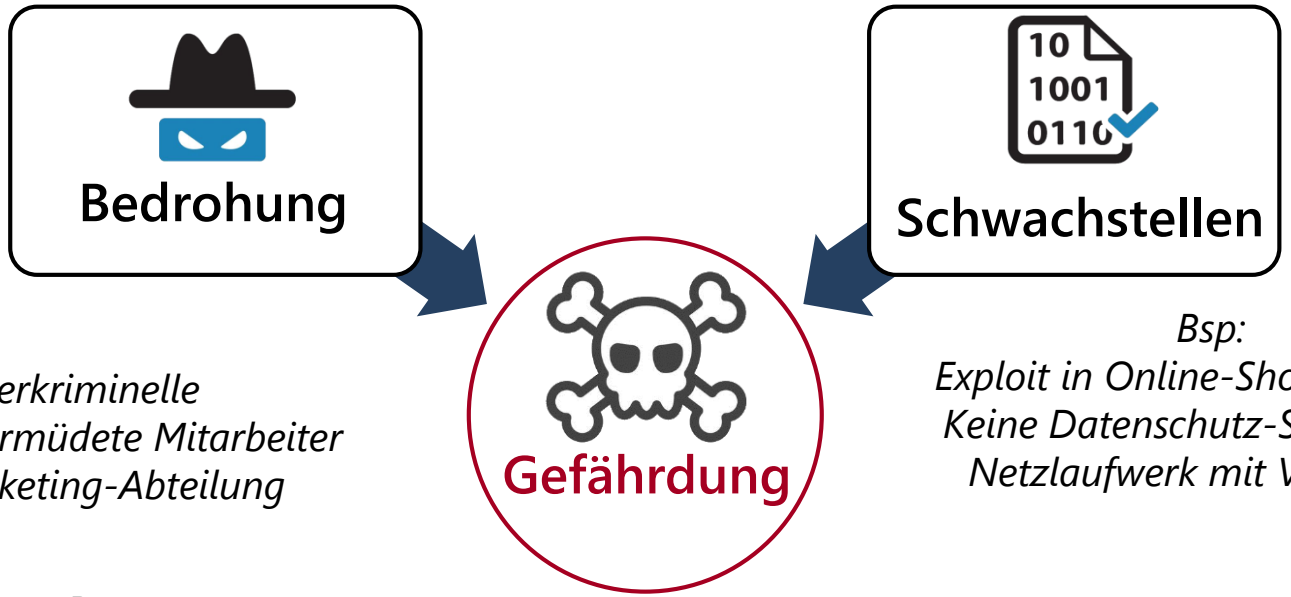
Bsp: Veröffentlichung von Teilnehmern eines Parteitages auf einer im Ausland gehosteten Internetplattform

Profilbildung von Aufenthaltsorten

Bsp: Unzulässige Zweckänderung von Daten eines PayAsYou-Drive Versicherers zur Marketing-Zwecken

III Sicherheit personenbezogener Daten

Risiko: Generischer Ansatz

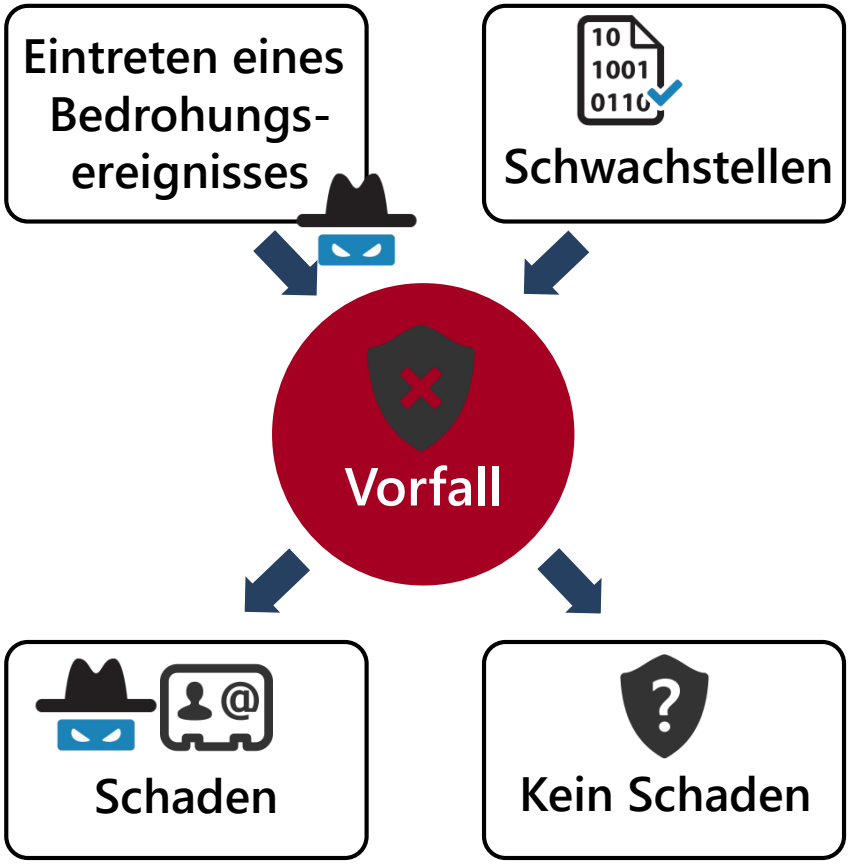


Bsp:
Cyberkriminelle
Übermüdete Mitarbeiter
Marketing-Abteilung

Bsp:
Exploit in Online-Shop-Software
Keine Datenschutz-Schulungen
Netzlaufwerk mit Vollzugriff

Bsp:
Online-Shop wird gehackt
Email-Versand mit 2000 Empfänger in CC
Einsatz von Facebook Custom Audience (mit großer gefundener Textdatei)

Risiko: Generischer Ansatz



Identitätsdiebstahl
Rufschädigung (Newsletter mit speziellem Inhalt)
Erweiterung des eigenen Facebook-Profils (mit ebenfalls speziellen Neigungen)

- *Glück gehabt:*

Kein Käufer im Darknet

- *Schaden ist immer individuell*

Offener Umgang mit speziellen Neigungen

- *Oder: Schaden tritt ein, ohne dies zu merken*

III Sicherheit personenbezogener Daten

Risiko: Generischer Ansatz

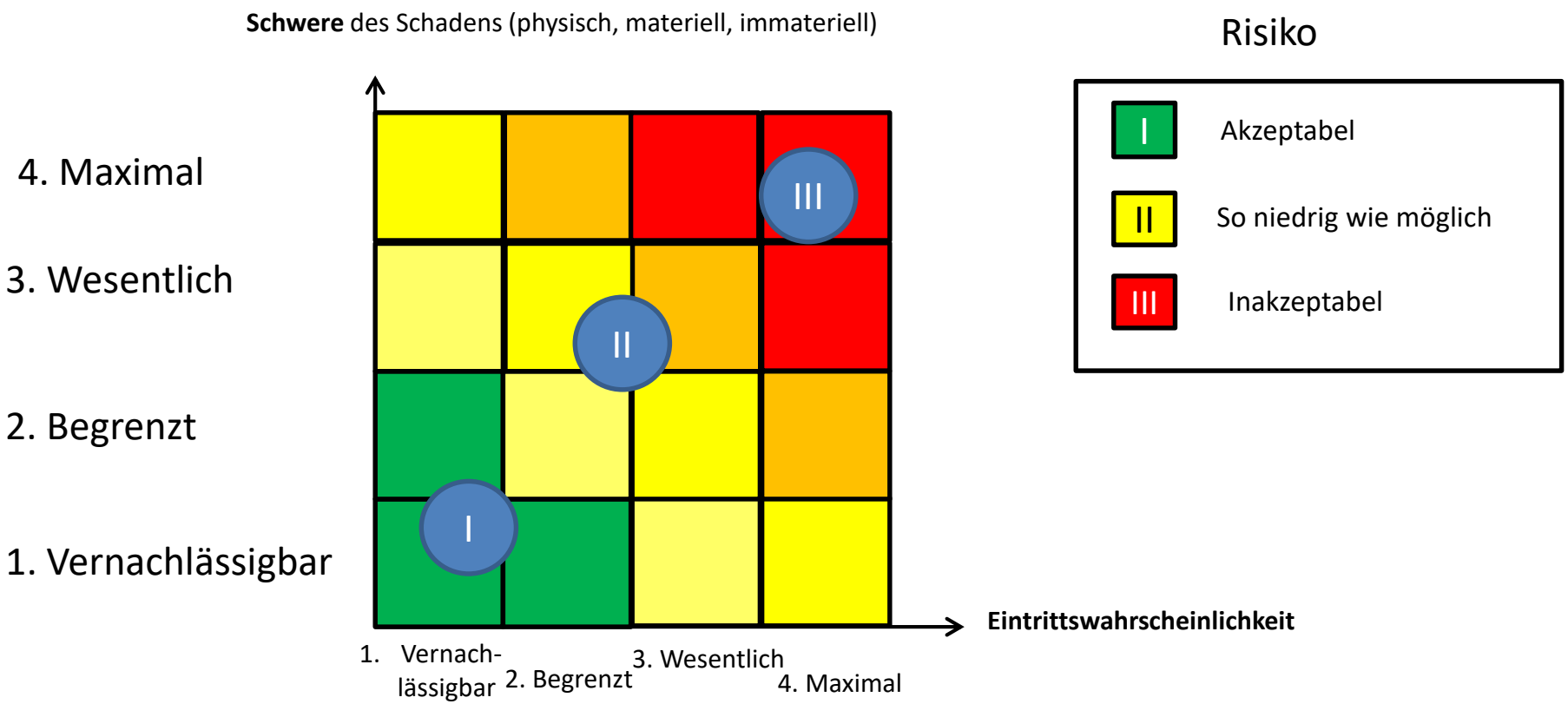
Risiko = Schaden x Eintrittswahrscheinlichkeit

Eine monetäre Berechnung eines Schadens im Kontext Datenschutz geht meistens nicht

Statt dessen kann es hilfreich sein, das Risiko in wenige Ausprägungen zu unterteilen, die auch die rechtlichen Konsequenzen der DS-GVO abbilden (z.B. Pflicht einer Datenschutzfolgeabschätzung bei hohem Risiko)

III Sicherheit personenbezogener Daten

Risiko: Eine Möglichkeit zur Bestimmung



Eintrittswahrscheinlichkeit und Risiko-Quellen

Nochmal: Ein **Risiko** ist ein möglicher Schaden, das immer in der Zukunft liegt.

Der **Schaden** kann bei der Annahme, dass „etwas schief geht“ abgeschätzt werden (z.B. Vernachlässigbar, Begrenzt, Wesentlich, Maximal).

Dazu werden **konkrete Verarbeitungstätigkeit** (z.B. Online-Shop, digitale Patientenakte, Bewerbungsverfahren,…) durch den Blickwinkel auf die „Rechte und Freiheiten“ bewertet

Eintrittswahrscheinlichkeiten beziehen sich damit immer auf **konkrete Bedrohungen**.
Die Ursache der Bedrohungen – die **Risiko-Quellen** – müssen dazu explizit betrachtet werden.
Blickwinkel der IT-Sicherheit: Angreifermodellierung

III Sicherheit personenbezogener Daten

Eintrittswahrscheinlichkeit und Risiko-Quellen

Bei der Sicherheit der Verarbeitung nach Artikel 32 wird der Blickwinkel für die Risiko-Quellen festgelegt:

Vernichtung	unbeabsichtigt
Verlust	unrechtmäßig
Veränderung	

Offenlegung von	unbefugt
Zugang zu	

Mögliche Risiko-Quellen
Cyberkriminelle/“Hacker“
Interner Administrator
Wettbewerber
„Normaler“ Mitarbeiter
Geschäfts-/Abteilungsleitung
Dienstleister
Staatliche Organisationen

III Sicherheit personenbezogener Daten

Eintrittswahrscheinlichkeit und Risiko-Quellen

Durch Verknüpfung von Risiko-Quellen und Schadensszenarien können Bedrohungen für **konkrete Verarbeitungstätigkeiten** modelliert werden:

Möglicher Schaden	Risiko-Quellen	Eintrittswahrscheinlichkeit (Beispiel)	Schadenshöhe (Beispiel)	Risiko
Diskriminierung durch fahrlässige Offenbarung interner Daten	„Normaler“ Mitarbeiter,	Vernachlässigbar	Vernachlässigbar	Akzeptabel
	Dienstleister	Wesentlich	Vernachlässigbar	So gering wie möglich
Identitätsdiebstahl in Online-Shop	Cyberkriminelle/“Hacker“	Maximal	Wesentlich	Inakzeptabel
	Interner Administrator	Wesentlich	Wesentlich	So gering wie möglich
Finanzieller Verlust durch Malware	Cyberkriminelle/“Hacker“	Wesentlich	Begrenzt	So gering wie möglich

Eintrittswahrscheinlichkeit und Risiko-Quellen

Weitere Beispiele

Möglicher Schaden	Risiko-Quellen	Eintrittswahrscheinlichkeit (Beispiel)	Schadenshöhe (Beispiel)	Risiko
Rufschädigung durch „Ausplaudern“ vertraulicher Informationen im Sportverein	Interner Mitarbeiter	Vernachlässigbar	Maximal	So gering wie möglich
Profilbildung von Aufenthaltsorten	Geschäfts-/Abteilungsleitung	Begrenzt	Maximal	So gering wie möglich

Auswahl von TOMs

Voraussetzung: Für eine konkrete Verarbeitungstätigkeit

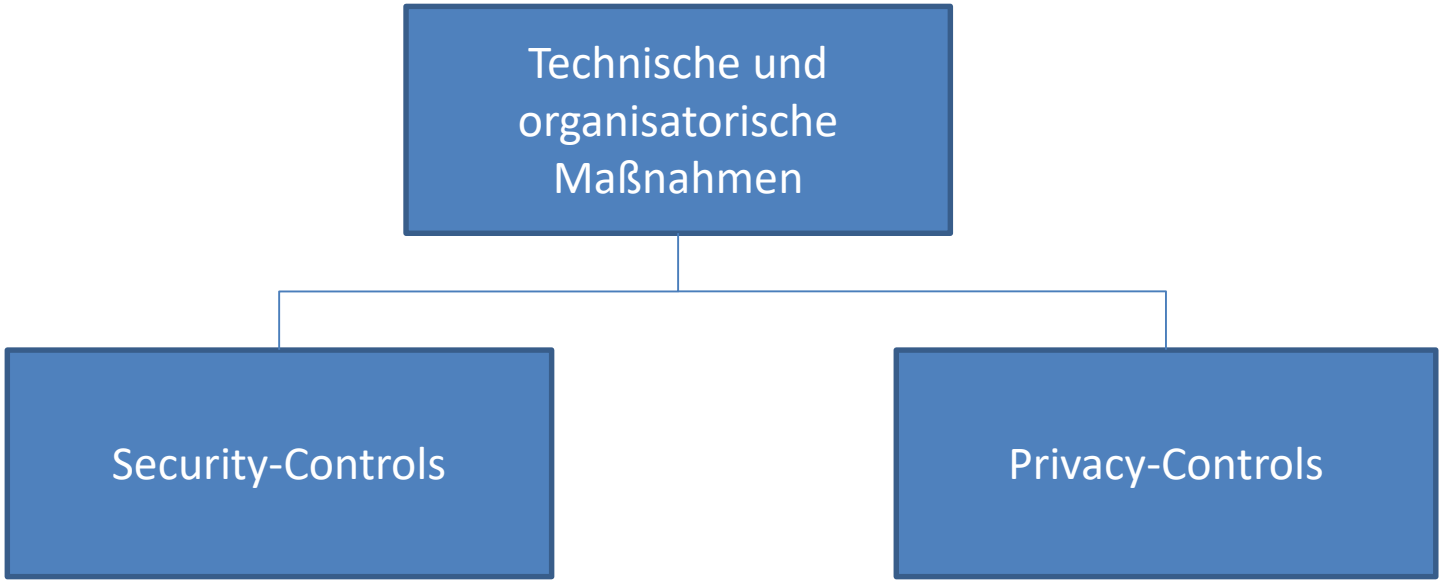
- Festlegung eines möglichen **Schadens**
- Ermittlung der **Risiko-Quellen**
- Abschätzung der **Eintrittswahrscheinlichkeiten**
- Bestimmung des **Risikos**

Für jedes Risiko, dass größer als „Akzeptabel“ ist:

- **Auswahl** und Umsetzung von geeigneten technischen und organisatorischen Maßnahmen
- Maßnahmen müssen **wirksam** sein
- Maßnahmen müssen **vollständig** sein
- Berücksichtigung zum **Stand der Technik**
- Berücksichtigung **Implementierungskosten**
- **Restrisiko**bewertung

III Sicherheit personenbezogener Daten

Auswahl von TOMs



- Schutzmaßnahmen der Informationssicherheit
- Angepasst auf die Verarbeitung personenbezogener Daten
- Fokus auf Vertraulichkeit, Integrität, Verfügbarkeit

- Schutzmaßnahmen des (technischen) Datenschutzes
- Explizit: Pseudonymisierung, Verschlüsselung
- Fokus auf Datenschutzgrundsätze (z.B. Datenminimierung, Zweckbindung, Transparenz,…)

Privacy & Security in ISO 29151 (Draft)

ISO 27001: Management process/requirements
ISO 29100: Privacy framework

ISO 27005: Security risk management

ISO 29134: Privacy impact assessment

ISO 27002: Code of practice for Information security controls

ISO 29151: Code of practice for PII protection

Nochmals TOMs

Guidelines bzw. Best-Practise zur Auswahl von technischen und organisatorischen Maßnahmen:

- ISO 27002 : Code of practice for Information security controls
- ISO 29151: Code of practice for PII protection
- IT-Grundschutz Kataloge des BSI
- Maßnahmenkatalog des Standard-Datenschutzmodells (ab 2017)
- ISACA, Control Objectives for Information and Related Technology (COBIT 5)
- OECD, Guidelines for the Security of Information Systems and Networks
- OWASP für Webanwendungen
- FedRamp (Security Controls)
- Eigene Maßnahmenlisten

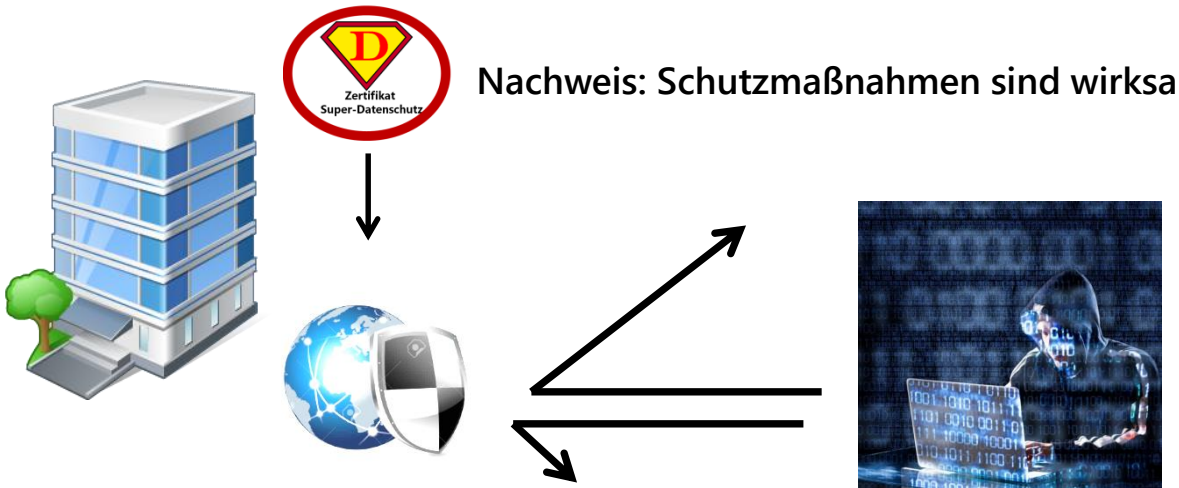
IV Nachweispflicht

Artikel 32: Zertifizierung und Code of Conduct

ABSCHNITT 5

VERHALTENSREGELN UND ZERTIFIZIERUNG

Zertifizierungen können als Faktor herangezogen werden, um die Einhaltung der „Sicherheit der Verarbeitung“ **nachzuweisen (Wichtig!).**



IV Nachweispflicht

Nachweis der Sicherheit durch Code of Conduct

CODE
of Conduct
...

Ähnliches „Werkzeug“ wie bei einer Zertifizierung.

Faktoren bei

Artikel / EG	**Code of Conduct**	**Zertifizierung**
Art.24: Datenschutzkonforme Datenverarbeitung	✓	✓
Art. 28: Auftragsdatenverarbeitung	✓	✓
Art. 32: Informationssicherheit	✓	✓
Art. 35: Datenschutzfolgeabschätzung	✓	✗
Art. 46 Drittlandtransfer	✓	✓

V Aufsichtsbehörden

Einschub in eigener Sache: Aufsichtsbehörden

Es schlagen nach der EU-DSGVO
zwei Herzen in der Brust
der Datenschützer

- Beraten
- Fördern
- Prüfen
- Sanktionieren

Artikel 83 Absatz 1: In jeden Fall sollten die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein.

VI Datenpannen

Umgang mit Datenpannen: Stand heute

Heute Meldepflichtig:

- Eingrenzung auf sehr sensible Daten

  +

- Feststellung, dass schwerwiegende Beeinträchtigungen drohen

Informationspflicht nach § 42a BDSG bei

- Besonderen Arten personenbezogener Daten
- Personenbezogene Daten von Berufsgeheimnisträgern
- Personenbezogene Daten die sich auf Straftaten / Ordnungswidrigkeiten beziehen
- Bank- und Kreditkartendaten
- Bestands-/Nutzungsdaten (§15a TMG)

- Betroffene müssen **unverzüglich** informiert werden
- zusätzlich: es drohen **schwerwiegende Beeinträchtigungen**

VI Datenpannen

Artikel 33: Meldung einer Datenpanne

Verletzung des Schutzes personenbezogener Daten

- Muss **unverzüglich**, spätestens nach 72 Stunden der **Aufsichtsbehörde** gemeldet werden
- **Ausnahme**: Verletzung führt voraussichtlich nicht zu einem Risiko für den Betroffenen

Morgen Meldepflichtig:

- Keine Eingrenzung auf sehr sensible Daten mehr
- Keine Feststellung mehr, dass schwerwiegende Beeinträchtigungen drohen
- Einzige Ausnahme:
  - voraussichtlich kein Risiko
  - Was bedeutet das? Verschlüsselung?

- **Auftragsverarbeiter** muss Verantwortlichen unverzüglich informieren

- **Nichtmeldung** Bußgeldbewährt **bis 10 Mio. Euro / 2 % Umsatz**

VI Datenpannen

DS-GVO und „Datenpannen“

Zentraler Punkt:
„*Verletzung des Schutzes personenbezogener Daten*“

Fokus auf (Artikel 4 Abs. 12):

Vernichtung	unbeabsichtigt
Verlust	unrechtmäßig
Veränderung	

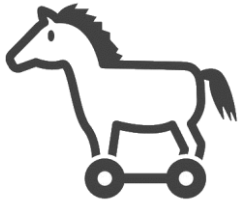
Offenlegung von	unbefugt
Zugang zu	

VI Datenpannen

Artikel 33: Meldung einer „Datenpanne“ an Aufsichtsbehörde

Beispiele für eine Meldepflicht

- **Hacking**
- **Verlust**
- **Diebstahl**
- **Fehlversand**
- **Softwarefehler**
- **Schadcode**
- **Fehlentsorgung**
- **Vernichtung Verlust**
- **Sonstiges?**



VI Datenpannen

Artikel 33: Meldung einer „Datenpanne“ an Aufsichtsbehörde

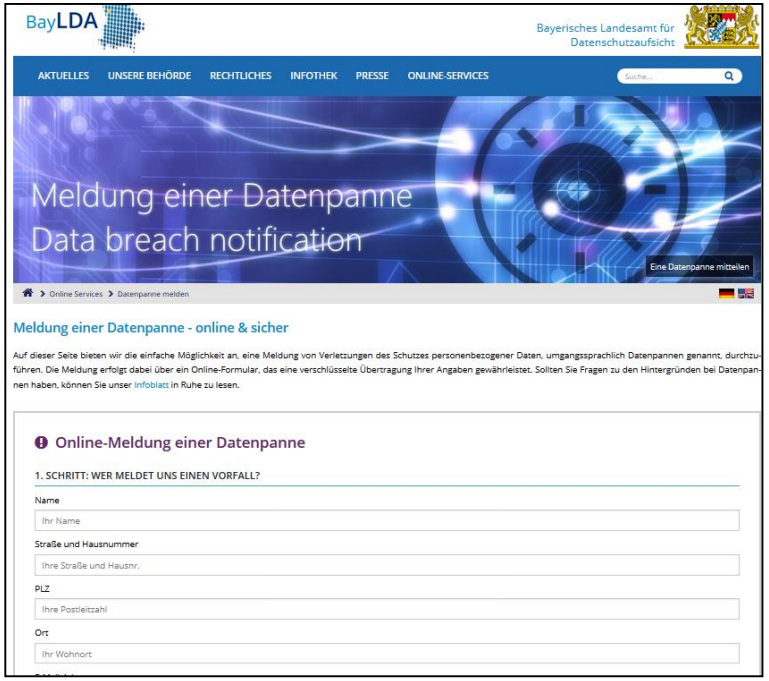
Inhalt der Meldung:

- **Art** der Verletzung (z.B. Diebstahl USB-Stick, Hacking Online-Shop, Fehlversand Arztbriefe,…)
- **Kategorien** Personen (z.B. Angestellte, Patienten, Kunden, Versicherte, Passanten,…)
- **Anzahl** Betroffene
- **Kategorien** personenbezogener Daten (z.B. Adresse, Bankverbindung, Gesundheitsdaten, Zugangsname/Passwort, Fotos, Standortdaten…)
- **Anzahl** Datensätze
- **Kontaktdaten** (DSB/weitere Ansprechpartner)
- Beschreibung der wahrscheinlichen **Folgen** für Betroffene
- Beschreibung der **Schutzmaßnahmen**, die nach dem Vorfall getroffen werden/wurden
- Maßnahmen zur **Schadenskompensation**
- **Dokumentation** des Vorfalls (auch für Aufsichtsbehörde)

VI Datenpannen

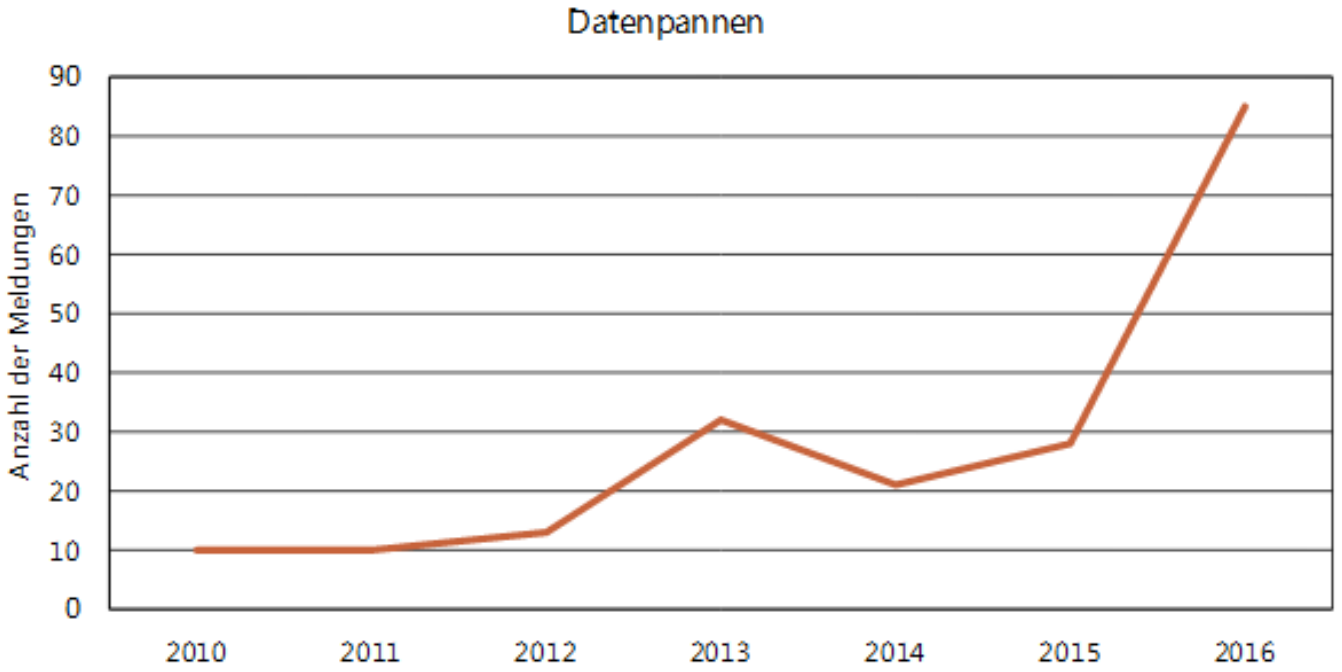
Artikel 33: Meldung einer „Datenpanne“ an Aufsichtsbehörde

Meldung zu kompliziert?
Dann einfach online melden (in Bayern):
https://www.lda.bayern.de/de/datenpanne.html



VI Datenpannen

Kurzer Einschub: Aktuelle Zahlen des BayLDA



Tätigkeitsbericht 2015/2016 abrufbar unter www.lda.bayern.de

VI Datenpannen

Artikel 33: Meldung einer „Datenpanne“ an Betroffene

- **Meldung**, sofern Vorfall voraussichtlich ein **hohes Risiko** für die Rechte und Freiheiten natürlicher Personen zur Folge hat
- Muss **unverzüglich** erfolgen
- In **klarer und einfacher Sprache** formuliert
- **Beinhaltet** mindestens:
  - Kontaktdaten (DSB/weitere Ansprechpartner)
  - Beschreibung der wahrscheinlichen Folgen für Betroffene
  - Beschreibung der Schutzmaßnahmen, die nach dem Vorfall getroffen werden/wurden
- Allerdings auch **keine** Meldung falls,
  - Daten (durch Verschlüsselung) unzugänglich gemacht wurden
  - Nach Vorfall Maßnahmen zur Risikosenkung ergriffen wurden ⇨ noch unklar, wie weit dies geht

VI Datenpannen

Artikel 33: Meldung einer „Datenpanne“ an Betroffene

- **Meldung**, sofern Vorfall voraussichtlich ein **hohes Risiko** für die Rechte und Freiheiten natürlicher Personen zur Folge hat
- Muss **unverzüglich** erfolgen
- In **klarer und einfacher Sprache** formuliert
- **Beinhaltet** mindestens:
  - Kontaktdaten (DSB/weitere Ansprechpartner)
  - Beschreibung der wahrscheinlichen Folgen für Betroffene
  - Beschreibung der Schutzmaßnahmen, die nach dem Vorfall getroffen werden/wurden
- Allerdings auch **keine** Meldung falls,
  - Daten (durch Verschlüsselung) unzugänglich gemacht wurden
  - Nach Vorfall Maßnahmen zur Risikosenkung ergriffen wurden ⇨ noch unklar, wie weit dies geht

Zusammenfassung

Vielen Dank für Ihre Aufmerksamkeit

Deutliche Schärfung der gesetzlichen Anforderungen

Datenschutz und Informationssicherheit Können (meist) zusammen ausgestaltet werden

Deutliche Steigerung der Meldungen an die Aufsichtsbehörden

Neu: Verstöße der „Sicherheit“ sind bußgeldbewährt

Zertifizierungen können (auch) zum Nachweis der „Sicherheit der Verarbeitung“ abgewendet werden