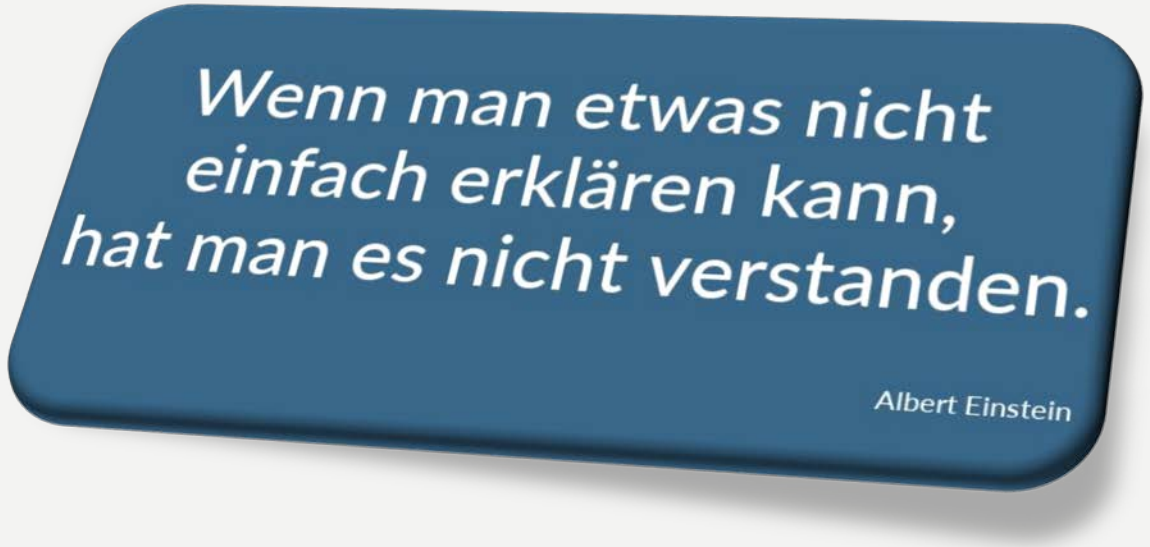
DATENSCHUTZGRUND-VERORDNUNG 679/2016/EU

NEUERUNGEN

BY RA.DR. PERNTHALER KLAUS

BOZEN, AM 17.06.2018

DSGVO
GDPR


Wenn man etwas nicht
einfach erklären kann,
hat man es nicht verstanden.
Albert Einstein


DSGVO

WAS BISHER ZU BEACHTEN GALT …

- Nationale Gesetzgebungen
  - Datenschutzkodex (G.v.D 196/2003)
  - Telekommunikationsgesetz
  - Italienischer Zivilgesetzkodex
- Nationale Aufsichtsbehörden

EU-DATENSCHUTZ-GRUNDVERORDNUNG (EU-DSGVO)

Gegenstand und Ziele

- Diese Verordnung enthält Vorschriften zum **Schutz natürlicher Personen** bei der Verarbeitung **personenbezogener Daten** und zum **freien Verkehr** solcher Daten.
- Diese Verordnung schützt die **Grundrechte und Grundfreiheiten natürlicher Personen** und insbesondere deren Recht auf Schutz personenbezogener Daten.
- Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener **Daten weder eingeschränkt noch verboten** werden.

WAS UNS NUN ERWARTET …

- Einheitlicher europäischer Rahmen
  - Verordnung 679/2016/EU – Datenschutzgrundverordnung

- Zeitrahmen
  - Am 24. Mai 2016 in Kraft getreten
  - Ab 25. Mai 2018 ist es das alleinig gültige Regelwerk

  - 06. Mai 2018: Frist für die Mitgliedsstaaten eigene Gesetze zur Anwendung der Verordnung zu erlassen

DATENSCHUTZ UND INFORMATIONELLE SELBSTBESTIMMUNG

– Einklang mit anderen Rechten

- Die Verarbeitung personenbezogener Daten sollte im Dienste der Menschheit stehen. Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden. Diese Verordnung steht im **Einklang mit allen Grundrechten** und **achtet alle Freiheiten und Grundsätze**, die mit der Charta anerkannt wurden und in den **Europäischen Verträgen verankert** sind, insbesondere Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, Schutz personenbezogener Daten, Gedanken-, Gewissens- und Religionsfreiheit, Freiheit der Meinungsäußerung und Informationsfreiheit, unternehmerische Freiheit, Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren und Vielfalt der Kulturen, Religionen und Sprachen.

WICHTIGE BEGRIFFE
ART. 4

1. Personenbezogene Daten:
   - Alle Informationen, die sich auf eine identifizierte oder identifizierbare **natürliche Person** beziehen
   - Die Person muss **direkt oder indirekt identifizierbar** sein
   - Z.B. IP Adressen, Accounts in Sozialen Netzwerken.

Verarbeitung

- Jeder mit oder ohne Hilfe von automatisierten Verfahren ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten.

WICHTIGE BEGRIFFE
ART. 4

2. Pseudonymisierung:
   - Verarbeitung von personenbezogenen 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

   - **NICHT „nur“ Anonymisierung**

WICHTIGE BEGRIFFE
ART. 4

3. Profiling:
   - Automatisierte Verarbeitung personenbezogener Daten, die darin besteht, dass die personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleitung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen

WICHTIGE BEGRIFFE
ART. 4

4. Sensible Daten:
   - Personenbezogene Daten aus denen erfolgen:
     - **Rassische und ethnische Herkunft**
     - **Politische Meinungen**
     - **Religiöse und weltanschauliche Überzeugungen**
     - **Gewerkschaftszugehörigkeit**
     - **Genetische Daten**
     - **Biometrische Daten zur eindeutigen Identifizierung von natürlichen Personen**
     - **Gesundheitsdaten**
     - **Daten zum Sexualleben oder zur sexuellen Orientierung**

WICHTIGE BEGRIFFE
ART. 4

5. Rechtmäßige Verarbeitung:
   - Einwilligung der betroffenen Person für die Verarbeitung für ein oder mehrerer Zwecke
   - Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist
   - Erfüllung einer rechtlichen Verpflichtung
   - Wahrung lebenswichtiger Interessen der betroffen Person
   - Wahrnehmung einer Aufgabe im öffentlichen Interesse/ Ausübung öffentlicher Gewalt
   - Wahrung berechtigter Interessen (z.B. Verwaltung eines Vereins ohne Gewinnabsichten, ONLUS)

5. Rechtmäßige Verarbeitung:

RECHTMÄßIGKEIT

- Die Rechtmäßigkeit orientiert sich neben den Prinzipien „Verhältnismäßigkeit“ (Art. 5 Abs. 1 lit. b), „Transparenz“ (Art. 5 Abs. 1 lit. a), „Datenminimierung“ (Art. 5 Abs. 1 lit. c), „Richtigkeit“ (Art. 5 Abs. 1 lit. d), „Speicherbegrenzung“ (Art. 5 Abs. 1 lit. c) und „Integrität und Vertraulichkeit“ (Art. 5 Abs. 1 lit. f), insbesondere an dem Prinzip der Zweckbindung (Art. 5 Abs. 1 lit. b).

WICHTIGE BEGRIFFE
ART. 4

6. Zustimmung:
   - Freiwillige für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

   - **Mit 16 Jahren möglich**

WICHTIGE BEGRIFFE
ART. 4

7. Verantwortlicher (ehem. Inhaber):
   - Bewertet Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen
   - Umsetzung technischer und organisatorischer Maßnahmen
   - Register der Verarbeitungstätigkeiten

   - **Die juristische Person oder der gesetzliche Vertreter**

   - **Gemeinsam für die Verarbeitung Verantwortliche?**

WICHTIGE BEGRIFFE
ART. 4

8. Auftragsverarbeiter (ehem. Verantwortliche):
   - Verarbeitung von personenbezogenen Daten im Auftrag eines Verantwortlichen/ Inhabers
   - Verantwortliche für die Umsetzung technisch und organisatorischer Maßnahmen
   - Rechtswirksamen Akt als Ernennung
   - Register der Verarbeitungstätigkeiten
   - Löschung oder Rückgabe aller Daten nach Beendigung der Ernennung

   - **meistens extern**

WICHTIGE BEGRIFFE
ART. 4

8. Auftragsverarbeiter (ehem. Verantwortliche):
   - Pflichten
     - Evtl. Nominierung DPO
     - Technische und organisatorische Mindeststandards
     - Warnpflicht
     - Haftung bei Nichteinhaltung
     - Risikoabschätzung
     - Verzeichnis der Verarbeitungstätigkeiten
     - Erfüllung der Betroffenenrechte

WICHTIGE BEGRIFFE
ART. 4

9. Verantwortlicher für den Datenschutz (DPO):
   - **Verpflichtend** für:
     - Öffentliche Behörden und öffentliche Stellen (außer Justizbehörden)
     - Organisationen deren Kerntätigkeit die umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht
     - **Umfangreiche Verarbeitung sensibler Daten** oder Gerichtsdaten
   - Ansonsten **freiwillig**
   - Intern oder extern
   - Kein Interessenskonflikt
   - Beratende Funktion, aber auch Aufsichtsfunktion

WICHTIGE BEGRIFFE
ART. 4

10. Prinzipien:

- **Rechtmäßigkeit**, Verarbeitung nach Treu und Glauben
- Transparenz
- **Zweckbindung**
- **Datenminimierung**
- Speicherbegrenzung
- **Richtigkeit**
- Integrität und Vertraulichkeit
- **Rechenschaftspflicht**

WICHTIGE BEGRIFFE
ART. 4

11. „Data breach“:
   - Verletzung des Datenschutzes (Diebstahl, Verlust, Manipulation)
   - Größtes Risiko intern
   - Meldung an Postpolizei und Aufsichtsbehörde
   - Meldung an Betroffene (wenn hohes Risiko für deren Rechte und Freiheiten)
   - Meldung an DPO

WICHTIGE BEGRIFFE
ART. 4

Rechte der betroffenen Personen:

- Transparente Information über die Ausübung seiner Rechte (Art. 12)
- Informationspflicht bei der Erhebung der Daten (Art. 13 f.)
- **Auskunftsrecht (Art. 15)**
- **Recht auf Berichtigung (Art. 16)**
- **Recht auf Widerruf (Art. 21)**
- **Recht auf Einschränkung der Verarbeitung (Art. 18)**
- **Recht auf Löschung (Art. 17)**
- Datenübertragbarkeit (Art. 20)
- Recht auf Benachrichtigung bei Datenmissbrauch/ Datenverlust

WICHTIGE BEGRIFFE

Rechte der betroffenen Personen:

- **Auskunftsrecht (Art. 15)**
  - Verarbeitungszwecke
  - Kategorien personenbezogener Daten
  - Kategorien der Empfänger
  - Speicherdauer
  - Betroffenenrechte
  - Kopie aller verarbeiteten Daten

  Antwort innerhalb 30 Tage ab Erhalt

WICHTIGE BEGRIFFE

Rechte der betroffenen Personen:

- **Recht auf Berichtigung (Art. 16)**
  - Unverzüglich vorzunehmen
  - Auch Integration nicht vollständiger Daten

WICHTIGE BEGRIFFE

Rechte der betroffenen Personen:

- **Recht auf Widerruf (Art. 21)**
  - Keine weitere Verarbeitung
  - Bereits stattgefundene Verarbeitung bleibt stehen
  - Marketing & Profiling: jederzeit Widerruf möglich

WICHTIGE BEGRIFFE

Rechte der betroffenen Personen:

- **Recht auf Einschränkung der Verarbeitung (Art. 18)**
  - Wenn die Richtigkeit bestritten wird, bis zur Klärung der Frage
  - Unrechtmäßige Verarbeitung
  - Verarbeitungszweck fehlt
  - Bei Einlegung eines Widerspruchs

WICHTIGE BEGRIFFE

Rechte der betroffenen Personen:

- **Recht auf Löschung (Art. 17)**
  - Verarbeitungszweck hat sich erfüllt
  - Widerruf der Einwilligung zur Datenverarbeitung
  - Widerspruch gegen die Datenverarbeitung
  - Unrechtmäßige Verarbeitung
  - Rechtliche Pflicht

WICHTIGE BEGRIFFE

Löschen der öffentlich zugänglichen Daten.

Ausnahme:

- Recht auf freie Meinungsäußerung
- Verteidigung vor Gericht
- Öffentliches, historisches oder statistisches Interesse,
- Rechtliche Pflicht zur Aufbewahrung

GDPR STEPS TO GENER....

HAUPTANFORDERUNG AUS DER DSGVO

Organisation

- Bestellung eines Datenschutzbeauftragten
- Technische & Organisatorische Maßnahmen

Prozesse

- Benachrichtigung bei Datenschutzverletzungen innerhalb 72 Stunden
- Datenschutzfolgeabschätzung

Technologie

- „ePrivacy by Design“ & „Privacy by Default“
- Stand der Technik

Recht

- Gesonderte Einwilligung pro Verwendungszweck
- Wiederruf der Einwilligung und „Recht aus Vergessenwerden“

BETRACHTUNG RELEVANTER GESETZE - BERUFSSCHWEIGEPFLICHTEN

GRUNDLAGEN DER RECHTMÄßIGKEIT DER DATENVERARBEITUNG

5. Kontrolle aller Informationsschreiben und Einverständniserklärungen
   - Nachbesserungen
   - Informationsschreiben vervollständigen und den betroffenen Personen zusenden
   - Einverständniserklärungen vervollständigen und dein Einwilligung der betroffenen Personen einholen

ZWECKBINDUNG UND DATEN-VERARBEITUNG FÜR EIGENE ODER FREMDE ZWECKE

DATENVERARBEITUNG IM AUFTRAG - RECHTE, PFLICHTEN, KONSEQUENZEN UND HAFTUNG

RECHTLICHE STELLUNG, AUFGABEN UND PFLICHTEN DER BEHÖRDLICHEN / BETRIEBLICHEN DATENSCHUTZBEAUFTRAGTEN

Brauche ich einen DPO (Art. 37 ff.)

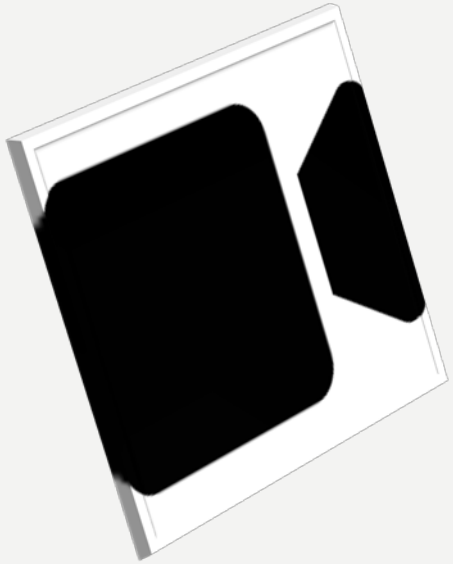
- Kontaktaufnahme
- Lebensläufe einholen
- Gespräche führen
- Ernennung
- Meldung an „Autorità Garante“

VORABKONTROLLE / DATENSCHUTZ-FOLGENABSCHÄTZUNG

Datenschutz- Folgeabschätzung (Art. 35)

- Nur wenn ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht
- Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der personenbezogenen Daten
- Zusammenarbeit mit DPO, wenn vorhanden
- Verpflichtend wenn:
  - Profiling: automatisierte sowie systematische und umfassende Bewertung persönlicher Aspekte
  - Umfangreiche Verarbeitung sensibler Daten und Gerichtsdaten
  - Systematische Überwachung öffentlich zugänglicher Bereiche
- Inhalt: Risikoabschätzung, Begründung der Verarbeitung, TOM, …

OPTISCH-ELEKTRONISCHE ÜBERWACHUNG (VIDEO) & GEOLOKALISIERUNG



INFORMATIONSPFLICHTEN

Schulung der Mitarbeiter

- Welche Daten werden verarbeitet?
- Welche Sicherheitsstandards sind einzuhalten?
- Was darf nicht gemacht werden?

- **Rat**: Einholen einer schriftlichen Verpflichtung zur Geheimhaltung der Daten und Einhaltung der Datenschutzbestimmungen

Informationspflicht gegenüber des Betroffen gemäss Art. 15

DOKUMENTATIONSPFLICHTEN (VERFAHRENSVERZEICHNIS)

Register der Verarbeitungstätigkeiten erstellen (Art. 30)

- Bestimmen der Verantwortlichen/ Inhabers
- Bestimmer der Verarbeitungszwecke
- Bestimmen der betroffenen Personen
- Welchen Dritten werden Daten übergeben (z.B. Lohnbüro)
- Findet Datenexport statt?
- Fristen für die Löschung von Daten
- Beschreibung der technischen und organisatorischen Maßnahmen

PRIVATE / BETRIEBLICHE INTERNET- UND E-MAIL-NUTZUNG

TECHNISCH-ORGANISATORISCHE MAßNAHMEN

Technische und organisatorische Maßnahmen:

- IST Zustand erheben (im Verzeichnis der Verarbeitungstätigkeiten)
- Verbesserungspotentiale bestimmen
- Umsetzungsplan erstellen
- Schulung der Mitarbeiter

IT-GRUNDSCHUTZ UND RISIKOFALLSTUDIE

Technische und organisatorische Maßnahmen:

- Privacy by design
- Privacy by default

- Durch Technikgestaltung und Voreinstellungen sollen nur jene Daten verarbeitet werden, die für den konkreten Anwendungsfall notwendig sind.
- Geeignete technische und organisatorische Maßnahme implementieren
- Datenschutzgarantien in der Entwicklungsphase
- Stand der Technik, Implementierungskosten, Art-Umfang-Umstände-Zwecke der Datenverarbeitung, Eintrittswahrscheinlich und mögliche Folgen

IT- / DATENSICHERHEIT

Technische und organisatorische Maßnahmen:

- Zugangskontrollen
- Datenträgerkontrollen
- Speicherkontrollen
- Benutzerkontrollen
- Zugriffskontrollen
- Übertragungskontrollen
- Transportkontrollen
- Wiederherstellbarkeit
- Zuverlässigkeit
- Datenintegrität

EXTERNER DATENSCHUTZ UND DATENSCHUTZAUDIT

HAFTUNG DER GESCHÄFTSFÜHRUNG

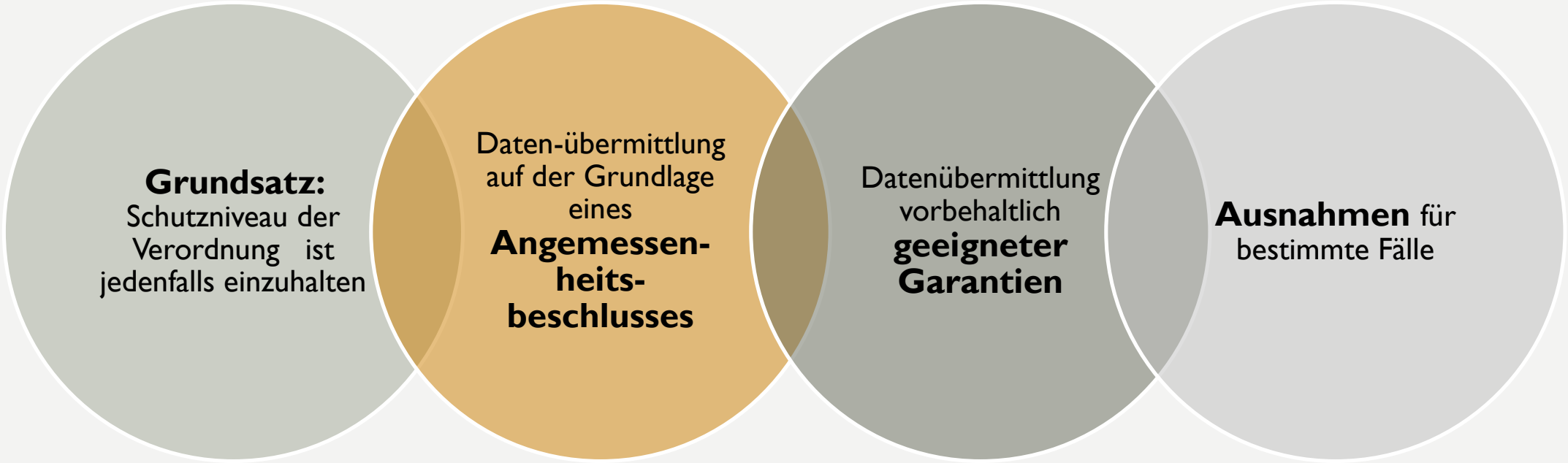
- **privacy by design / privacy by default (Artikel 25):**
  durch **Technikgestaltung** und **Voreinstellungen** sollen nur jene Daten verarbeitet werden, die für den konkreten Anwendungsfall notwendig sind,
  dazu sind geeignete technische und organisatorische Maßnahmen zu implementieren (zB. **Pseudonymisierung**)
  Datenschutzgarantien müssen schon in der ersten Entwicklungsphase „*eingebaut*“ werden
  Berücksichtigung des **Stands der Technik**, **Implementierungskosten**, Art/ Umfang/ Umstände und Zwecke der **Verarbeitung** sowie der unterschiedlichen **Eintrittswahrscheinlichkeit** und **Schwere** der Risiken für die Rechte und Freiheiten

HAFTUNG DES BETRIEBLICHEN DATENSCHUTZBEAUFTRAGTEN

- Die Regelung erfolgt durch die DSGVO 679/2016

DATENTRANSFER UND TRANS PORTABILITÄT EU-US PRIVACY SHIELD

GRENZÜBERSCHREITENDE DATENVERARBEITUNG (ARTIKEL 44FF)



BESCHWERDERECHTE - VERFAHREN

- **Parallelverfahren** (Artikel Nr. 77 und 78): Beschwerde sowohl vor den Aufsichtsbehörden als auch vor Gerichten möglich
- **Verbandsklagebefugnis** (Artikel Nr. 80) für non-profit Organisationen
- **Schadenersatz** (Artikel 82) sowohl für materiellen als auch immateriellen Schaden
  - **Solidarhaftung** im Falle mehrerer Schädiger
  - **Achtung: Verantwortlichkeit des Auftragsverarbeiters**

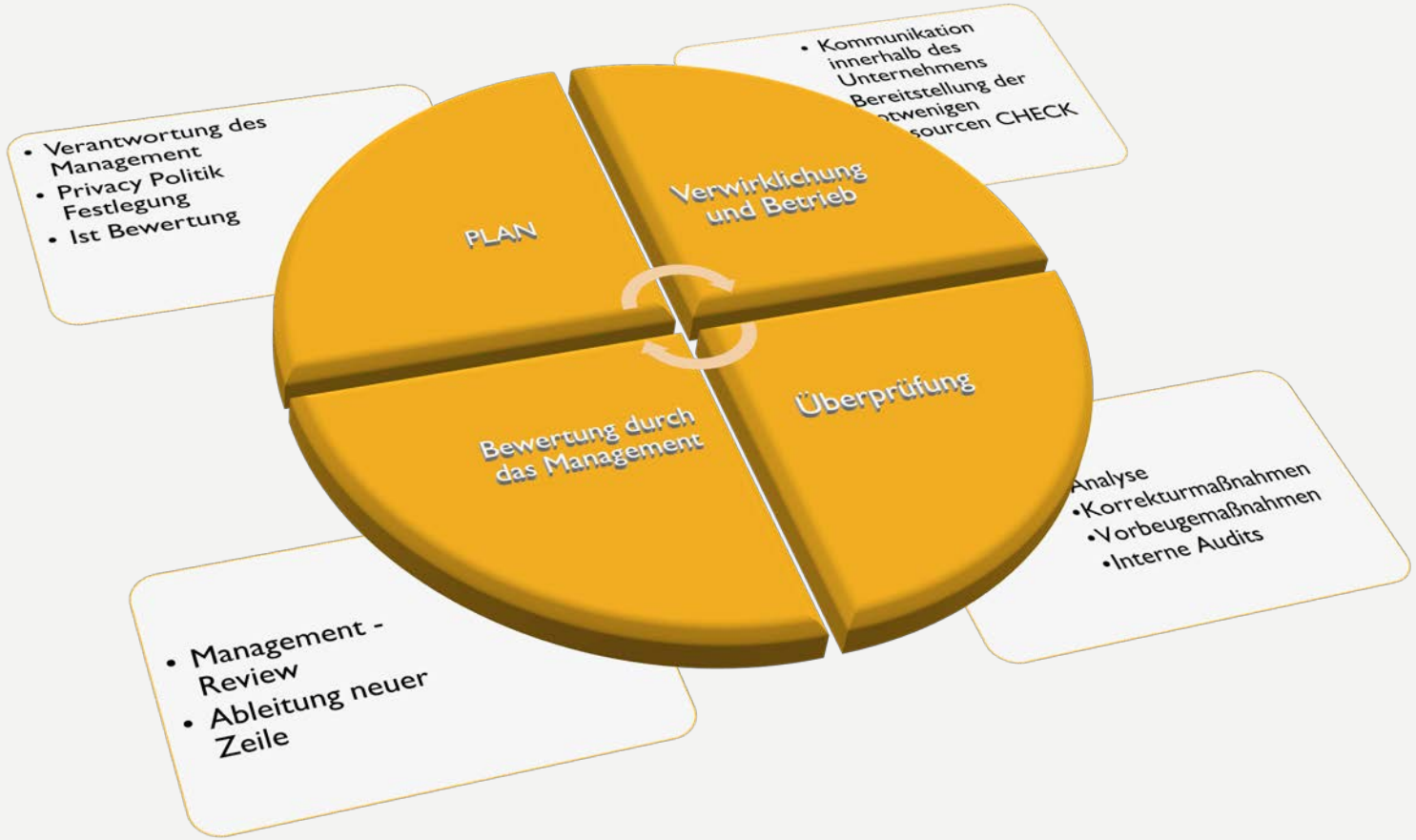
STRAFEN

- zusätzlich zu den weitgehenden **Ermittlungs-**, **Straf-** sowie **Beratungs- und Konsultationsrechten** der Aufsichtsbehörde kann sie auch **Verwaltungsstrafen** (Artikel 83 ff) festlegen.

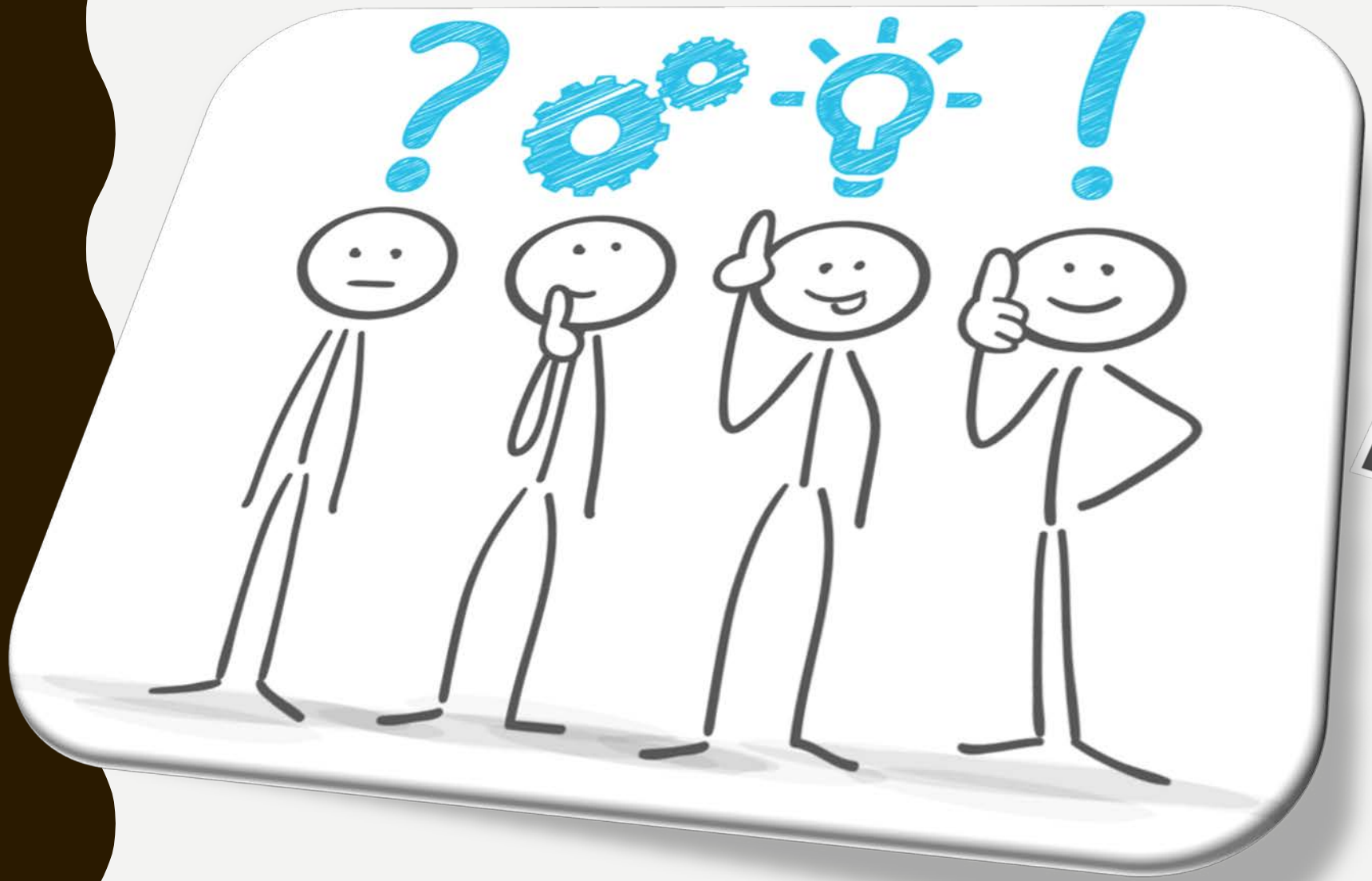
- Strafen können im schlechtesten Fall bis zu **20 Millionen oder 4% des Jahresumsatzes weltweit** betragen, je nach dem was sich als höher herausstellt;

- zusätzlich können Ministerien weitere Vorschriften über wirksame, verhältnismäßige und abschreckende Sanktionen für Verstöße festlegen;

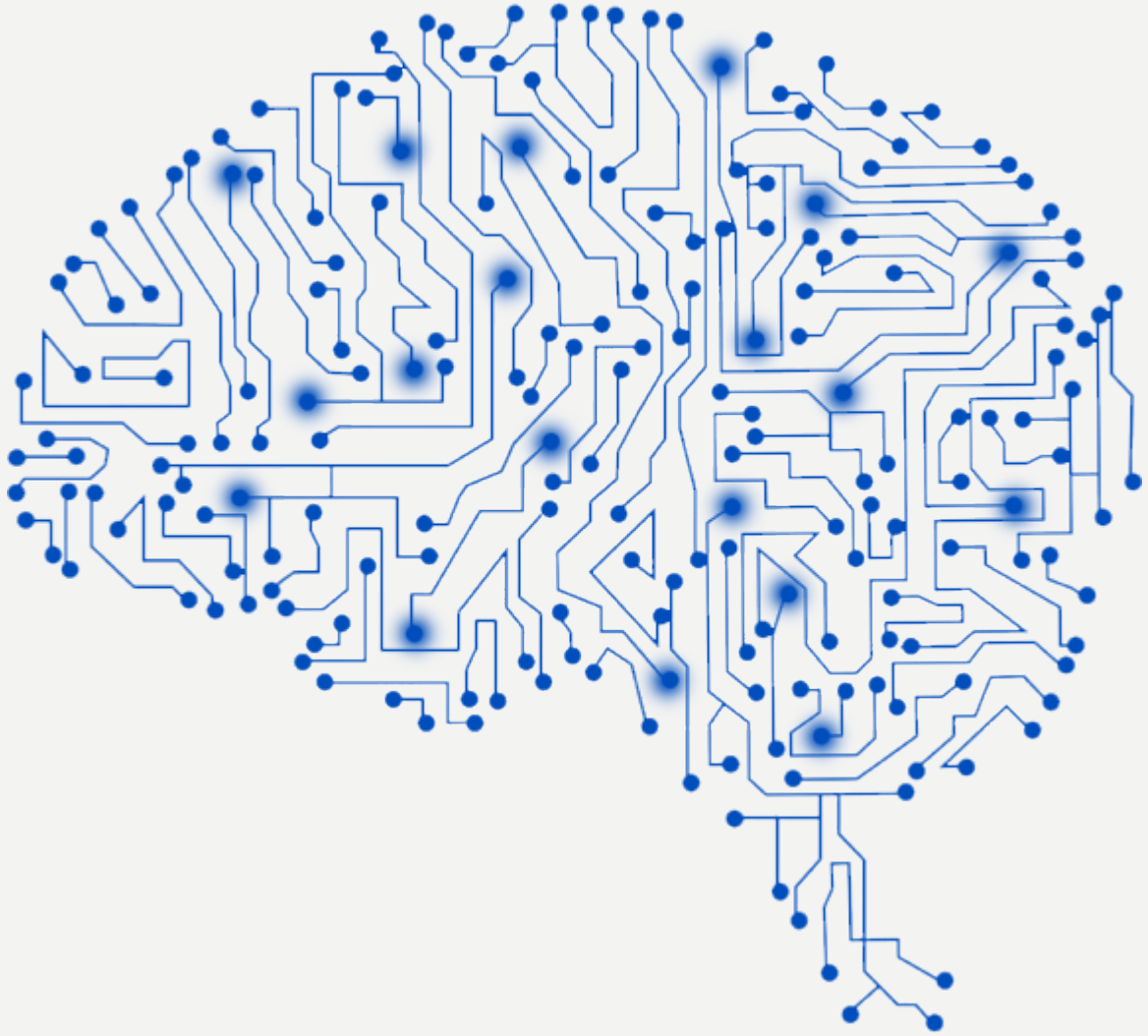
PRAKTISCHE UMSETZUNG DES DSGVO



ABSCHLIEßEND …



- Fragen
- Anregungen
- Vorschläge



DANKE FÜR IHRE ZEIT

Behandle jeden so, wie du selbst behandelt werden möchtest…..
auch seine Daten!

IFK Consulting GmbH

Vittorio Veneto Straße 67

39042 Brixen

Tel. 0472 831 107

klaus.pernthaler@ifkconsulting.com