# Datenschutzgrundverordnung - DSGVO

Was braucht ein Unternehmen,
um auf der (rechts-)sicheren Seite zu sein?

## Haftungsausschluss

Die vorliegende Unterlage stellt lediglich einen Überblick über das vorgetragene Thema dar.

Sie erhebt keinen Anspruch auf Vollständigkeit, gibt teilweise die Meinung der Autoren wieder und kann keinesfalls die Beratung im Einzelfall und die Konsultation diverser Berater (Rechtsanwälte, Steuerberater, sonstige Berater) ersetzen.

Der Inhalt wurde unter größtmöglicher Sorgfalt erstellt, ist jedoch ohne Gewähr.

Eine Haftung aus der vorliegenden Unterlage ist ausgeschlossen.

# Allgemeines




## EU-**D**aten**S**chutz**G**rund**V**er**O**rdnung

Das neue europäische
Weltbild …

## Warum Datenschutz?


"Wer nichts zu verbergen hat,
hat auch nichts zu befürchten!"



## Warum Datenschutz?

- ✓ Man gebe mir sechs Zeilen, geschrieben von dem redlichsten Menschen, und ich werde darin etwas finden, um ihn aufhängen zu lassen … (Kardinal Richelieu 1585-1642)

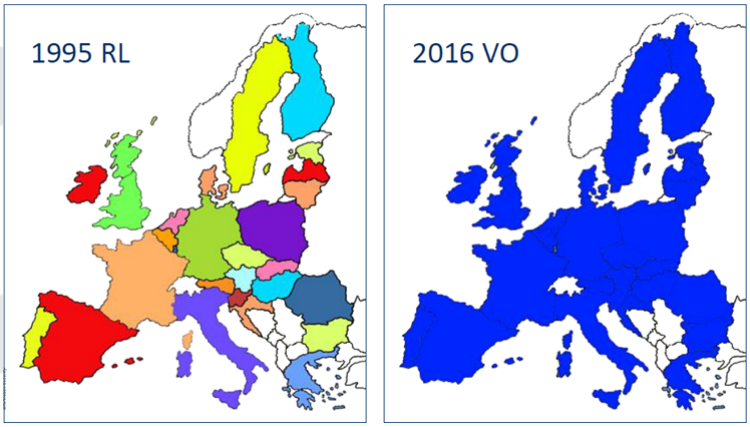
## Daten sind das Öl des 21. Jahrhundert …




## Daten sind das Öl des 21. Jahrhundert …

## Wie hat sich die DSGVO entwickelt?

- ✓ 1995 - 1. Richtlinie -> 28 Datenschutzgesetze
- ✓ 2016 - 1. Verordnung -> 1 Datenschutzgesetz







## Wie hat sich die DSGVO entwickelt?

- ✓ 04. Mai 2016 Amtsblatt der EU veröffentlicht
- ✓ 25. Mai 2016 DSGVO ist in Kraft getreten
- ✓ **25. Mai 2018** DSGVO ist anwendbar

# Rechtlicher Überblick/Hintergründe




# Grundrecht auf Datenschutz

- ✓ § 1 DSG 2000: „Jedermann hat […] Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht […]
- ✓ § 1 Abs 2 DSG 2000: „Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig […]

**Verhältnis Datenschutz und Informationsfreiheit**

Ein Eingriff in das Grundrecht ist nur dann zulässig, wenn im Rahmen einer Verhältnismäßigkeitsprüfung die Interessenabwägung zugunsten der legitimen Informationsinteressen ausgeht.

## Um wessen Daten geht es?

- ✓ Daten natürlicher Personen
  - ✓ Mitarbeiter
  - ✓ Kunden
  - ✓ Lieferanten
  - ✓ Kooperationspartner




## Welche Daten sind erfasst?

- ✓ **Personenbezogene Daten**
  - ✓ Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen
  - ✓ zB Name, Kontaktdaten, Kleidergröße, Einkommen, SV-Nr, Charaktereigenschaften etc
- ✓ **Sensible Daten**
  - ✓ Rassistische und ethnische Herkunft
  - ✓ Politische Meinungen
  - ✓ Religiöse oder weltenanschauliche Überzeugungen
  - ✓ Gewerkschaftszugehörigkeit
  - ✓ Genetische oder biometrische Daten
  - ✓ Gesundheitsdaten
  - ✓ Sexuelle Orientierung

## Welche Daten sind erfasst?

- ✓ Pseudonymisierung
  - = *Verarbeitung personenbezogener Daten in der Weise, dass Rückidentifizierung nur durch Heranziehung zusätzlicher Informationen möglich ist*
  - → DSG-VO **ist** anwendbar!
- ✓ Anonymisierung
  - = *Rückidentifizierung ist nicht mehr möglich*
  - → DSG-VO **ist nicht** anwendbar!




## Welche Daten sind nicht erfasst?

- ✓ Daten juristischer Personen
- ✓ Betriebswirtschaftliche Kennzahlen
- ✓ Controlling-Kennzahlen
- ✓ Kennzahlen zur Teilnahme an Schulungen
- ✓ …

## Was ist Datenverarbeitung?

- ✓ Verarbeitung als weitgefasster Begriff
  - ✓ Erheben / Erfassen
  - ✓ Speicherung
  - ✓ Verwendung
  - ✓ Weitergabe / Verbreitung
  - ✓ Löschen / Vernichtung etc

  → zB Erstellung einer Kundendatei, Datenaufnahme zur Erstellung einer Rechnung, Mitarbeiterdatenbank

- ✓ Verarbeitung im Rahmen der Tätigkeit einer Niederlassung in der EU
- ✓ Verarbeitung findet **überall** statt (zB Cloud)




## Datenverarbeitung im Geschäftsleben Beispiel Mitarbeiter

1. 

Name
Geburtsdatum
Informationen über Ausbildung
dzt. Berufstätigkeit

2. 

Verfassen des Dienstvertrages

3. 

Ablage des schriftlichen Vertrages in physischen Ordner
Aufnahme Geburtsdatum in interne Geburtstagsliste

## Datenverarbeitung im Geschäftsleben
## Beispiel Mitarbeiter

Natürliche oder juristische Person, die über Zwecke und Mittel der Datenverarbeitung entscheidet und für entstandene Schäden haftet

Verantwortlicher

Interesse an Informationen

Natürliche Person, deren Daten verarbeitet werden

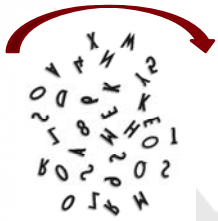
Betroffener

Interesse an Datenschutz




## Personen & Interessen im Geschäftsleben

Verantwortlicher: IT-DL



Auftragsverarbeiter

Betroffener: Kunde

## Auftragsverarbeiter

= natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet

- ✓ Verarbeitung auf **Weisung des Verantwortlichen**
- ✓ **Verwendungszweck** bestimmt Verantwortlicher
- ✓ Auftragsverarbeiter entscheidet über Mittel (technisch und organisatorisch)
- ✓ IT-Dienstleister als Auftragsverarbeiter?




## Auftragsverarbeiter – Wer kann das sein?

- ✓ Natürliche oder juristische Person
- ✓ Niederlassung **in oder außerhalb der EU**

**Ausländischer Auftragsverarbeiter:**
zulässig, wenn zusätzlicher Aspekt vorliegt, nämlich

- ✓ Angemessenheitsbeschluss (Art 45 DSG-VO) oder
  - ✓ Feststellung durch Beschluss der EK
- ✓ Geeignete Garantien (Art 46 & 47 DSG-VO) ansonsten
- ✓ ausdrückliche Zustimmung des Betroffenen (Art 49 DSG-VO)

## Auftragsverarbeiter – Vertrag

- ✓ **Schriftlicher** Vertrag
- ✓ **Standardvertragsklauseln** der EK oder der Aufsichtsbehörde
- ✓ **Inhalt** des Vertrages:
  - ✓ Gegenstand & Dauer der Verarbeitung
  - ✓ Art und Zweck der Datenverarbeitung
  - ✓ Rechte & Pflichten des Auftragsverarbeiters sowie des Auftraggebers
  - ✓ Unterauftragsverhältnisse
  - ✓ Mitteilungspflichten
  - ✓ Weisungen
  - ✓ Beendigung des Auftrags & Kündigungsrechte
  - ✓ Vergütung
  - ✓ Haftung
  - ✓ Vertragsstrafe




## Auftragsverarbeiter-Sub-Auftragsverarbeiter

- ✓ **Schriftliche Zustimmung** des Verantwortlichen
  - ✓ Gesonderte Genehmigung eines konkreten Sub
  - ✓ Allgemeine Genehmigung mit Vorabinformation des Verantwortlichen über konkreten Sub → Möglichkeit eines Einspruches
- ✓ Auftragsverarbeiter trifft **Prüfpflicht** gegenüber Sub hinsichtlich dessen Zuverlässigkeit
- ✓ Auftragsverarbeiter **haftet** gegenüber Verantwortlichen für Einhaltung der Pflichten des Sub

## Auftragsverarbeiter – Verarbeitungs-verzeichnis I

= schriftliches Verzeichnis über Verarbeitungstätigkeiten, die im Auftrag eines Verantwortlichen durchgeführt werden (Art 30 DSG-VO)

- ✓ Zweck: Kontrollmöglichkeit der Aufsichtsbehörde
- ✓ Verkürztes Verzeichnis

- ✓ kein Verzeichnis, wenn
  1. < 250 Mitarbeiter und
  2. Verarbeitungstätigkeit kein Risiko für Betroffene und
  3. Nur gelegentliche Verarbeitungstätigkeiten und
  4. Keine Verarbeitung sensibler Daten




## Datenschutzrechtliche Grundsätze I

- ✓ **Rechtmäßigkeit**
  - ✓ Darf ich Daten überhaupt verarbeiten?
  - ✓ Einwilligung, Erfüllung einer vertraglichen Verpflichtung, Wahrung berechtigter Interessen des Verantwortlichen, Erfüllung einer Rechtsvorschrift?

- ✓ **Transparenz**
  - ✓ Kunde muss wissen, was mit seinen Daten passiert

- ✓ **Zweckbindung**
  - ✓ Aufnahme der Daten des Mitarbeiters im Dienstvertrag → wofür? (Vertragszweck!)
  - ✓ Weiterverarbeitung (Alumniveranstaltung?)

## Datenschutzrechtliche Grundsätze II

- **Richtigkeit**
  - Sind die Daten des Kunden/Mitarbeiters richtig und aktuell?
- **Verhältnismäßigkeit**
  - Datenverarbeitung zur Verwirklichung eines legitimen Zwecks?
  - Datenverarbeitung als mildestes Mittel?
  - Interessenabwägung: Recht auf Information vs Recht auf Datenschutz




## Datenschutzrechtliche Grundsätze III

- **Koppelungsverbot**
  - Kundenkarte für Prozente?
- **Datenminimierung**
  - Welche Daten brauche ich wirklich? (SV-Nr?!)
- **Speicherbegrenzung**
  - Wie lange darf ich Daten des Kunden/Mitarbeiters speichern?
  - Beschränkung auf das unbedingt erforderliche Mindestmaß
  - Generelle Speicherfrist von 7 Jahren (Aufbewahrungsfrist nach § 132 BAO)
  - Gewährleistung / Schadenersatz: 3 – maximal 30 Jahre

## Datenschutzrechtliche Grundsätze IV

- ✓ **Integrität** und **Vertraulichkeit**
  - ✓ Wer kann intern auf die Daten zugreifen?
    - → Geeignete technische und organisatorische Maßnahmen
- ✓ **Rechenschaftspflicht**
  - ✓ Unternehmen muss Grundsätze einhalten und Nachweis darüber führen - Verfahrensverzeichnis
- ✓ Recht auf **"Vergessenwerden"**




## Sonderfälle

- ✓ **Bildverarbeitung (Foto, Video (inkl. Ton)**
  - ✓ Kennzeichnungspflicht
  - ✓ Verantwortlicher muss hervorgehen
  - ✓ Keine Meldepflicht mehr (ab 25.5.2018)
  - ✓ Zulässigkeit gegeben
    - ✓ Lebenswichtiges Interesse
    - ✓ Gesetzliche Erlaubnis
    - ✓ Im Einzelfall, wenn ein überwiegend berechtigtes Interesse vorliegt, im Rahmen der Verhältnismäßigkeit (vorbeugender Schutz für private Liegenschaften, öffentliche Bereiche ….)
    - ✓ Einwilligung erteilt
  - ✓ Generelles Recht am Bild – Zustimmung ist im Zweifel erforderlich (auch konkludent?)

## Datenschutzfolgenabschätzung – Was ist das und warum soll ich diese durchführen?

- ✓ Bewertung der möglichen **Risiken** nach Art, Umfang, Umständen, verfolgten Zwecke und Ursachen und Prüfung von **Maßnahmen**, Garantien und Verfahren zur Eindämmung der Risiken
- ✓ **Geldbuße** bis zu € 10 Mio oder 2% des weltweiten Konzernjahresumsatzes bei Unterlassung




## Datenschutzfolgenabschätzung – Wann muss ich diese durchführen?

- ✓ Verwendung neuer Technologien
- ✓ Neuartige Verarbeitungsvorgänge
- ✓ Verarbeitung großer Datenmengen
- ✓ Datenverarbeitung einer großen Personenanzahl
- ✓ Verarbeitung sensibler Daten
- ✓ Systematische Überwachung öffentlicher Bereiche

## Datenschutzfolgenabschätzung – Was habe ich zu beachten?

- ✓ Systematische **Beschreibung** der geplanten Verarbeitungsvorgänge und Angabe des Zwecks
- ✓ Prüfung der **Notwendigkeit** und **Verhältnismäßigkeit** des Verarbeitungsvorganges zum verfolgten Zweck
- ✓ Datenschutzfolgenabschätzung für mehrere ähnliche Verarbeitungsvorgänge
- ✓ Angabe der geplanten **Abhilfemaßnahmen**
- ✓ **Vorgaben der Aufsichtsbehörde** beachten
- ✓ Rat des **Datenschutzbeauftragten** einholen
- ✓ Rechtssichere Dokumentation

Ergebnis: hohes Risiko → Konsultation der Aufsichtsbehörde (DSB)

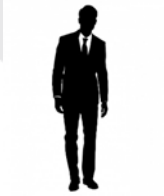



## Sanktionen/Haftung–Hintergrundinformation

- ✓ **Verschärfung** der Verpflichtungen der Verantwortlichen
- ✓ Massive **Erhöhung** der Strafbestimmungen
- ✓ Geldbußen sollen **wirksam, verhältnismäßig** und **abschreckend** sein
- ✓ Keine Erleichterungen mehr für KMU
- ✓ Verwarnungen nur mehr begrenzt zulässig

## Wer haftet?

Verantwortlicher
- Geschäftsführung?
- Vorstand ?



Auftragsverarbeiter

Entlastung durch Bestellung eines Datenschutzbeauftragten

Haftung des IT-DL für datenschutzrechtliche Verfehlungen des Kunden




## Auftragsverarbeiter - Haftung

- ✓ Haftungsauslösendes Ereignis
  - ✓ **Verstoß** gegen auferlegte **Pflichten**
  - ✓ **Nichtbeachtung** / Zuwiderhandeln rechtmäßig erteilter **Weisungen**
- ✓ Folgen
  - ✓ **Solidarische Haftung** mit Verantwortlichem
    - ✓ Regressanspruch gegenüber Verantwortlichem

## Entlassung aus Haftung durch Bestellung eines Datenschutzbeauftragten?

- ✓ Nein!
- ✓ Keine persönliche Haftung des Datenschutzbeauftragten
- ✓ Verantwortlicher bzw. Auftragsverarbeiter haftet weiterhin




## Sanktionen: Geldbuße

- ✓ Bis zu **€ 10 Mio** oder 2% des weltweiten Konzernjahresumsatzes
  - ✓ Unterlassene Datenschutzfolgenabschätzung
  - ✓ Keine Bestellung eines Datenschutzbeauftragten trotz Verpflichtung
- ✓ Bis zu **€ 20 Mio** oder 4% des weltweiten Konzernjahresumsatzes
  - ✓ Verstoß gegen Grundsätze der Verarbeitung
  - ✓ Verstoß gegen Voraussetzungen der Einwilligungserklärung
  - ✓ Verstoß gegen die Informationspflicht

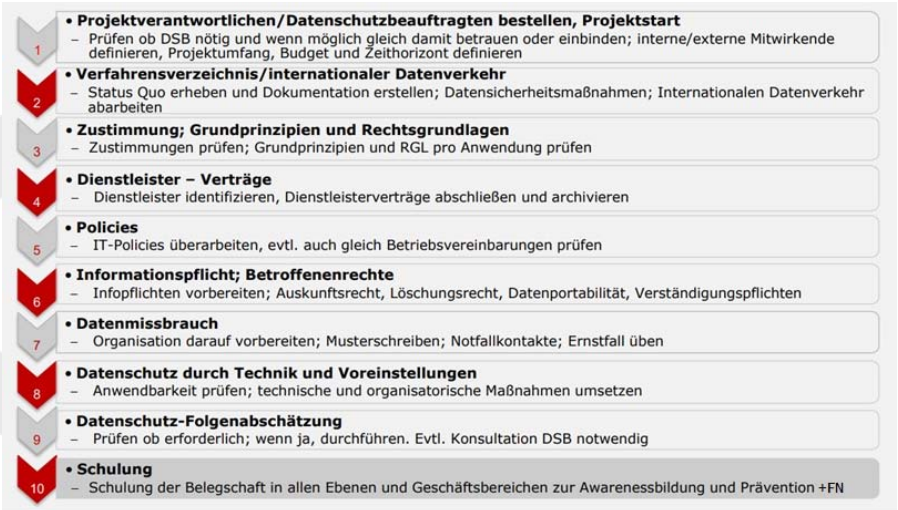
## Wer straft?

- ✓ Erste Instanz Datenschutzbehörde
  - ✓ Auf jeden Fall im Beschwerdefall
  - ✓ Kündigen sich vorher an
  - ✓ Mitwirkungspflicht
- ✓ Beschwerde beim Bundesverwaltungsgericht
- ✓ Zur Klärung von ausschließlich Rechtsfragen – Revision beim Verwaltungsgerichtshof




## Verantwortungen, Datenschutzbeauftragter, Prozess

## Fahrplan zur Umsetzung der DSGVO Verpflichtungen







## Datenschutzbeauftragter - Wann muss ich einen bestellen?

- ✓ Kerntätigkeit besteht in umfangreichen, regelmäßigen, systematischen **Überwachungen**
  - ✓ Banken; Versicherungen; Unternehmen, die Bewertungsplattformen und Vergleichsportale betreiben; IT-Dienstleister
- ✓ Kerntätigkeit besteht in umfangreicher Verarbeitung **sensibler Daten**
  - ✓ Behörden / öffentlichen Stellen
  - ✓ Sonstige gesetzliche Anordnung
- ✓ Sonstige gesetzliche Vorgaben

## Datenschutzbeauftragter - Wer kann das sein?

- ✓ **Interner** Datenschutzbeauftragter
  - ✓ Mitarbeiter des Verantwortlichen
  - ✓ Mitarbeiter des Auftragsverarbeiters
- ✓ **Externer** Datenschutzbeauftragter
  - ✓ Datenschutzbeauftragter als Auftragsverarbeiter
  - ✓ Abschluss eines Dienstleistungsvertrages




## Verzeichnis von Verarbeitungstätigkeiten Dokumentation sämtlicher Prozesse

## Verzeichnis von Verarbeitungstätigkeiten

- ✓ Das Verzeichnis von Verarbeitungstätigkeiten ersetzt ab 25.5.2018 die Meldepflicht iSd §§ 17ff DSG 2000 (https://dvr.dsb.gv.at/at.gv.bka.dvr.public/DVRRecherche.aspx)
- ✓ Die bis dato meldepflichtigen Informationen entsprechen zu einem Gutteil jenen Informationen, die auch im Verfahrensverzeichnis zu führen sind
- ✓ Die Verantwortliche (Ihr Unternehmen) und der Auftragsverarbeiter (zB etwaige Dienstleister) haben ein Verzeichnis der Verarbeitungstätigkeiten zu führen, die beinhaltet u.a.:
  - ✓ Beschreibung des Zwecks der Datenverarbeitung
  - ✓ Beschreibung der Betroffenen und der verwendeten Datenarten
  - ✓ Datenempfänger, Dienstleister und die vertragliche Grundlage sowie die Dokumentation der geeigneten Garantien (Standardvertragsklauseln)
  - ✓ Löschfristen und Speicherdauer
  - ✓ Getroffene Datensicherheitsmaßnahmen




## Verarbeitungsverzeichnis für jede Verarbeitung

- ✓ Verantwortlicher
- ✓ Datenkategorien
- ✓ Zweck(e)
- ✓ Auftragsverarbeiter
- ✓ Übermittlung der Daten an andere Verantwortliche – Zwecke
- ✓ Verarbeitung auf Grundlage einer Einwilligung (Kopie der Einwilligungserklärung?)
- ✓ Kopie der Datenschutzmitteilung (sofern vorhanden)
- ✓ Datensicherheitsmaßnahmen

## Empfänger der Daten

- ✓ Banken
- ✓ Rechtsvertreter im Geschäftsfall
- ✓ Wirtschaftstreuhänder
- ✓ Gerichte im Anlassfall
- ✓ Verwaltungsbehörden im Anlassfall
- ✓ Fremdfinanzierer (zB Leasing)
- ✓ Mitwirkende Vertrags- und Geschäftspartner
- ✓ Versicherungen im Anlassfall
- ✓ Provider (IT Dienstleister)
- ✓ …




## Stammdatenblatt

| Stammdaten des Verantwortlichen | | |
|---|---|---|
| **Angaben zum Verantwortlichen** | | |
| Name | | |
| Anschrift | | |
| Firmenbuchnummer | | |
| DVR-Nummer | | |
| **zuständige Aufsichtsbehörde(n)** | | |
| Name | | |
| Anschrift | | |
| Kontaktdaten | | |
| **Vertretung des Verantwortlichen** | | |
| Name | | |
| Kontaktdaten | | |
| **Betriebsrat** | **Name** | **Kontaktdaten** |
| Zentralbetriebsrat | | |
| Arbeiter | | |
| Angestellte | | |

# Verzeichnis der Verarbeitungen

| Verzeichnis aller Verarbeitungen | | |
|---|---|---|
| **Lfd. Nr.** | **Name der Verarbeitung** | **Beschreibung der Verarbeitung** |
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |
| 11 | | |
| 12 | | |
| 13 | | |
| 14 | | |
| 15 | | |
| 16 | | |
| 17 | | |
| 18 | | |




# Detailerhebung

| Detailerhebung | | |
|---|---|---|
| **Angaben zur Verarbeitung** | | |
| **Verarbeitung** | | |
| **Lfd. Nr.** | | |
| **Zweck der Verarbeitung** | | |
| **Erhebungsdetails** | | |
| **Auskunftspersonen** | **Name der Auskunftspersonen im Inteview** | **Abteilung, Funktion** |
| | | |
| **Prüfung der Verarbeitung** | | |
| **Datum der letzten Prüfung** | | |
| **Datum der aktuellen Prüfung** | | |
| **Datum der nächsten Prüfung** | | |
| **Risikoabschätzung** | | |
| **Datenschutz-Folgenabschätzung** | | |
| **Risikoklassifikation** | | |
| **Datenschutzklasse** | | |
| **Verarbeitungsklasse** | | |
| **Erlaubnistatbestände** | | |
| **Rechtgrundlage der Verarbeitung** | | |
| **besondere Kategorien personenbezogener Daten** | | |
| **Zweckbindung** | | |
| **Datenminimierung** | | |
| **Richtigkeit** | | |
| **Speicherbegrenzung** | | |
| **Integrität und Vertraulichkeit** | | |
| **Auftragsgebundenheit** | | |
| **Zuständigkeiten, Verantwortung** | **zuständige Rolle/Person/Abteilung** | **Name** |
| **fachlich verantwortlich** | | |
| **technisch zuständig** | | |

## Technische und Organisatorische Massnahmen - TOM

- ✓ Zutrittskontrollen: Schlüssel, Alarmanlage,…
- ✓ Zugangskontrolle: Kennwörter, Verschlüsselungen,…
- ✓ Zugriffskontrolle: Berechtigungen
- ✓ Weitergabekontrolle: Verschlüsselungen, …
- ✓ Eingabekontrolle: Protokolle,…
- ✓ Verfügbarkeitskontrolle: Virenschutz, Firewall,…
- ✓ Evaluierungsmassnahmen: Mitarbeiterschulungen, Datenschutzmanagement,….
- ✓ …




## Rechtlicher Überblick zu Informationspflichten und Einwilligung

## Rechtfertigungsgründe für Datenverarbeitung

- ✓ Erfüllung eines **Vertrages**
- ✓ **Gesetzliche** Verpflichtungen (BAO, etc…)
- ✓ **Berechtigte Interessen** des Verantwortlichen
- ✓ **Einwilligung**




## Warum muss ich informieren?

- ✓ **Geldbuße** von bis zu € 20 Mio oder 4% des weltweiten Jahreskonzernumsatzes
- ✓ Grundsatz der **Transparenz**

## Worüber habe ich zu informieren?

- ✓ Name und Kontaktdaten des Verantwortlichen
- ✓ ggf Kontaktdaten des Datenschutzbeauftragten
- ✓ Verarbeitungszweck und Rechtsgrundlagen
- ✓ zB Newsletter, Kundenkarte, Cookies, Werbung Dritter, Gewinnspiele
- ✓ Empfänger der Daten / Absicht der Datenübermittlung an Drittland
- ✓ Dauer der Datenspeicherung
- ✓ Betroffenenrechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch
- ✓ Möglichkeit des Widerrufs der Einwilligung
- ✓ Allfällige Interessenabwägung




## Wo und wie habe ich zu informieren?

- ✓ Präzise, leicht zugänglich und **verständlich**
- ✓ Klare und **einfache Sprache**
- ✓ **Schriftlichkeit**
  - ✓ Website: eigene datenschutzrechtliche Rubrik (Impressum nicht ausreichend)
  - ✓ Franchisevertrag: Datenaufnahme bereits im Zuge der Startgespräche
  - ✓ Arbeitsvertrag
  - ✓ Bsp: Datenschutzerklärung

## Der Weg aus der Misere - Einwilligungserklärung

- ✓ Wenn Datenverarbeitung nicht schon aufgrund anderer Grundlage zulässig ist, unbedingt Einwilligungserklärung einholen!

- ✓ Andere Grundlagen / Erlaubnistatbestände
  - ✓ Erfüllung einer vertraglichen Verpflichtung
  - ✓ Wahrung berechtigter Interessen des Verantwortlichen
  - ✓ Erfüllung einer rechtlichen Verpflichtung




## Einwilligungserklärungen

- ✓ **Freiwilligkeit**
  - ✓ Beachte Kopplungsverbot
- ✓ Aufklärung über **Datenart**
- ✓ Aufklärung über **Verarbeitungszweck**
- ✓ **Verständlich** und leicht zugängliche Form
- ✓ **Klare und einfache Sprache**
- ✓ Eindeutige **Abgrenzung** von anderen Vertragsklauseln
- ✓ **Widerrufsmöglichkeit**

## Einwilligungserklärungen - Form

- ✓ schriftlich
- ✓ mündlich
- ✓ ausdrücklich
- ✓ konkludent (zB Nicken)

Verarbeitung sensibler Daten: ausdrückliche Einwilligung




## Einwilligungserklärungen – Praxistipps

- ✓ **Schriftliche** Einwilligungserklärungen
- ✓ **Überprüfung** bislang verwendeter Zustimmungserklärungen
- ✓ Einholung neuer, **angepasster** Einwilligungen
- ✓ **Überarbeitung** der Einwilligungserklärungen in bestehenden Musterverträgen, Formularen etc

## Welche Rechte hat der Betroffene?

- ✓ Recht auf **Auskunft**
- ✓ Recht auf **Berichtigung** und **Einschränkung**
- ✓ Recht auf **Löschung** / Recht auf „Vergessenwerden"
- ✓ Recht auf **Widerspruch**

**Erfüllung der Rechte:**

Frist: 1 Monat ab Einlangen
2 Monate bei komplexen Fällen (ABER: Verständigung binnen 1 Monat über Gründe)




## Wie muss die Antwort aussehen?

- ✓ **Schriftlich** (Betroffener kann bei ausreichendem Identitätsnachweis mündliche Beantwortung verlangen)
- ✓ Klare, einfache und **verständliche** Sprache
- ✓ **Übermittlung** folgender Informationen
  - ✓ Kopie der Daten (E-Mails, Datenbankauszüge etc)
  - ✓ Konkret verarbeitete Daten
  - ✓ Verarbeitungszweck
  - ✓ Empfänger
  - ✓ Geplante Speicherfrist
  - ✓ Herkunft der Daten
- ✓ **Belehrung** über weitere Betroffenenrechte

## Data Breach – Was tun bei Datenpannen?

= *Verlust der vollständigen Kontrolle über die Daten und auch darüber, was mit diesen Daten passiert*

- ✓ Physischer, materieller oder immaterieller **Schaden** des Betroffenen
- ✓ Datenverlust durch **ungewollte** Panne oder grobe Fahrlässigkeit
  - ✓ zB aufgrund Softwarefehler sind Daten für andere Nutzer sichtbar; Versenden eines E-Mails mit Sichtbarkeit aller Empfänger; fehlender Passwortschutz; E-Mail aufgrund Namensähnlichkeit an falschen Empfänger
- ✓ **Vorsätzlich** herbeigeführte Datenpanne
  - ✓ zB Hacking, unzulässige Datenweitergabe




## Was tun bei einer Datenpanne?

## Was ist noch zu beachten?

- ✓ Telekommunikationsgesetz
  - ✓ Gilt unabhängig von der DSGVO
  - ✓ Anrufe ohne Einwilligung zu Werbezwecken (cold calls) sind unzulässig
  - ✓ Werbemails ohne vorherige Zustimmung zu Werbezwecken sind weiterhin unzulässig, wenn diese zu Direktmarketing verwendet werden oder an mehr als 50 Adressaten gehen
  - ✓ Absender darf nie unterdrückt werden
  - ✓ Zulässige Mails nach TKG
    - ✓ Kontaktinfo aus eine Vertrag bekannt
    - ✓ Nachricht zur Direktwerbung eigener ähnlicher Produkte
    - ✓ Einfache Opt Out Möglichkeit
    - ✓ Kein Eintrag in der Robinson Liste
- ✓ Erlaubnis zur Datenverarbeitung nach DSGVO ist davon unabhängig – Einwilligung nach DSGVO!!!!




## Abschließende Tipps

- ✓ Erstellung datenschutzrelevanter **Richtlinien**
- ✓ Interne **Schulungen** und **Schulungen der Kunden**
- ✓ Durchführung von **Audits**
- ✓ **Schnelle Reaktion** auf Zwischenfälle
- ✓ **Bearbeitung von Anfragen** von Betroffenen
- ✓ **Weiterführende Unterlagen der WKO**
  - ✓ https://www.wko.at/branchen/handel/datenschutzgrundverordnung-in-handelsunternehmen.html

mesonic
mit sicherheit ein gewinn

# Vielen Dank!

# Bis zum nächsten Mal!

**info@mesonic.com** **www.mesonic.com**