Die EU-Datenschutz-Grundverordnung

Eva-Maria Himmelbauer, BSc
Josef Himmelbauer, zert. DSB

Cloudcompany GmbH, A-2070 Retz, Kremserstraße 8
Tel. +43 2942 20670, Email: Info@Cloudcompany.at

Members of ARGE DATEN & privacyofficers

Die neue Datenschutz-Grundverordnung

- Neues Datenschutzregime tritt ab 25. Mai 2018 in Kraft
- Regelt den Schutz personenbezogener Daten

- Ist bindend für alle EU Mitgliedsstaaten

Sanktionen (Art 83 DSGVO)

- Strafrahmen bis EUR 10 Mio (2% des weltweiten Jahresumsatzes)

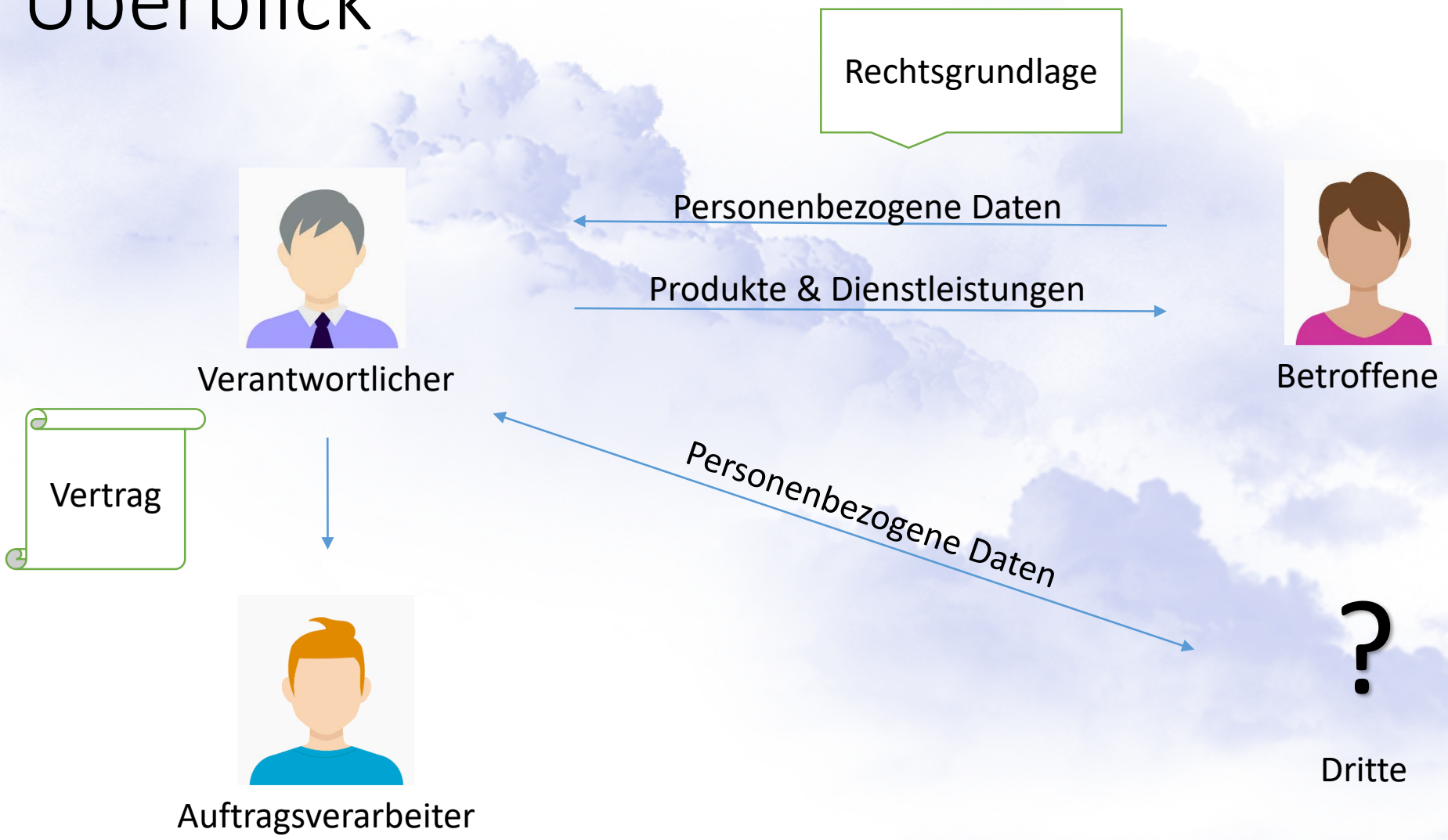
  -> Verletzung von Pflichten der Verantwortlichen

- Strafrahmen bis EUR 20 Mio (4% des weltweiten Jahresumsatzes)

  -> Verletzung von Rechten betroffener Personen

- Zuständige Strafbehörde ist die Datenschutzbehörde (früher Bezirkshauptmannschaft oder Magistrat)

Überblick


Rechtsgrundlage
Personenbezogene Daten
Produkte & Dienstleistungen
Verantwortlicher
Betroffene
Vertrag
Personenbezogene Daten
?
Auftragsverarbeiter
Dritte

Personenbezogene Daten

Personenbezogene Daten: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen

- Bspw. Name, Adresse, Geburtsdatum, Bankdaten, KFZ-Kennzeichen, IP-Adresse, Cookies, Bild

Besondere Kategorien („sensible Daten“): rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische & biometrische Daten, Gesundheitsdaten, sexuelle Orientierung

- Bspw. SVNr, Krankenstände, Religionsbekenntnis, …

Personenbezogene Daten

Datenschutzgesetz ist ein Verbotsgesetz!

Ausnahme:

- Verwendung im lebenswichtigen Interesse der Betroffenen
- Gesetzliche Ermächtigung oder rechtliche Verpflichtung
  - bspw. Arbeitszeitgesetz, Kollektivvertrag,
- Überwiegende berechtigte Interessen (nicht sensible Daten)
  - z.B. Vertragserfüllung, vorvertragliche Maßnahmen, Direkt Marketing bei bestehenden Kunden
- Zustimmung der Betroffenen liegt vor
- Daten sind öffentlich oder anonym

Einwilligungserklärung

„**Der Vertragspartner stimmt zu, dass seine persönlichen Daten, nämlich** … *(die Datenarten genau aufzählen, z.B. Fotos.)* **zum Zweck der** … *(genaue Zweckangabe, z.B. Darstellung auf der Internetseite www.cloudcompany.at und auf der Facebook-Seite www.facebook.at/cloudcompany)* **bei der Firma** *Cloudcompany GmbH* **verarbeitet werden und die Daten** … *(die Datenarten genau aufzählen, z.B. nämlich Namen, Tätigkeit, Fotos)* **zum Zweck der** … *(genaue Zweckangabe, z.B. der Darstellung auf …)* **an** … *(genaue Angabe des Übermittlungsempfängers, z.B. Werbeagentur, Facebook)* **weitergegeben werden.**

Diese Einwilligung kann jederzeit bei … *(Angabe der entsprechenden Kontaktdaten)* **widerrufen werden**.“

Datenschutzgrundsätze

Gelten für jede Verarbeitung:

- Rechtmäßigkeit, Fairness und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Pflichten des Verantwortlichen

- **Informationspflichten**
- *Bestellung Datenschutzbeauftragter*
- **Führung eines Verzeichnisses** über Verarbeitungstätigkeiten
- *In besonderen Fällen Folgenabschätzung über Verarbeitungen mit hohem Risiko für Grund- & Freiheitsrechte*
- **Verträge mit Auftragsverarbeitern**
- **Wahrung der Betroffenenrechte**: Informationspflicht, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung
- **Technische und organisatorische Maßnahmen** zum Schutz personenbezogener Daten
- **Data-Breach-Notification**: Information an Behörde innerhalb 72 Stunden

Informationspflichten bei der Erhebung

Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgendes mit:

- Namen und Kontaktdaten des Verantwortlichen (und ggf seiner Vertreter)
- *ggf Kontaktdaten des Datenschutzbeauftragten*
- Verarbeitungszwecke und Rechtsgrundlagen der Verarbeitung (bei berechtigtem Interesse Erläuterung dieser)
- ggf Empfänger der Daten
- Übermittlung an Drittland oder eine internationale Organisation (inkl. Hinweis auf Angemessenheitsbeschlusses der Europäischen Kommission, geeignete Garantien oder verbindliche internen Datenschutzvorschriften)

Informationspflichten bei der Erhebung

- Dauer der Datenspeicherung bzw. Kriterien für die Festlegung der Dauer
- Hinweis auf Betroffenenrechte
- Bei Einwilligung die Möglichkeit des Widerrufs
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte
- *ggf über das Bestehen automatisierter Entscheidungsfindung (inkl. Informationen über die involvierte Logik und die Tragweite der Entscheidung z.B.: Profiling)*
- *Beabsichtigte Weiterverarbeitung für andere Zwecke*

Informationspflichten

- bei Mitarbeiter – im Arbeitsvertrag (Personalführung, Lohnabrechnung, Arbeitszeitaufzeichnung, …)
- Endkunde – im Kaufvertrag, Mietvertrag, etc., auf der Homepage, in AGBs oder vorliegend im Geschäftslokal
- Geschäftspartner – im Vertrag, auf der Homepage oder in AGBs

-> https://dsgvo-informationsverpflichtungen.wkoratgeber.at/

Datenschutzbeauftragter

Eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten ist für Unternehmen nur in folgenden Fällen vorgesehen, wenn

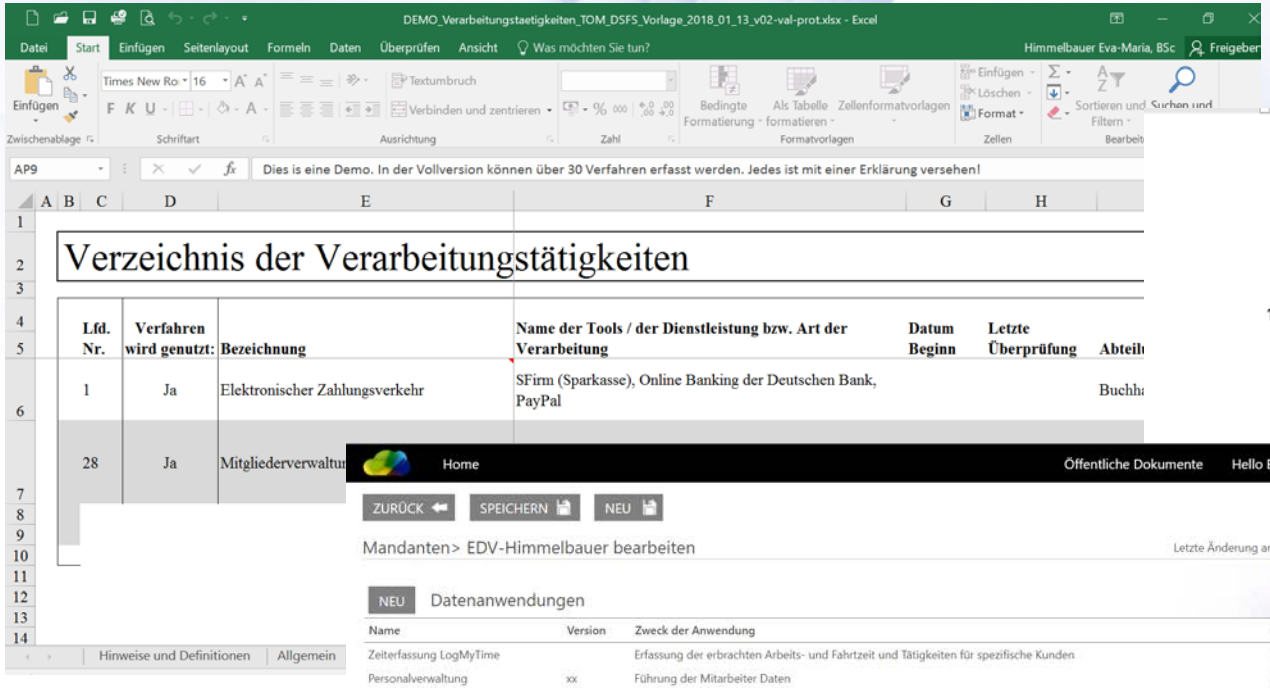
- die **Kerntätigkeit** in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfanges und/oder ihrer Zwecke eine **umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen** erforderlich machen

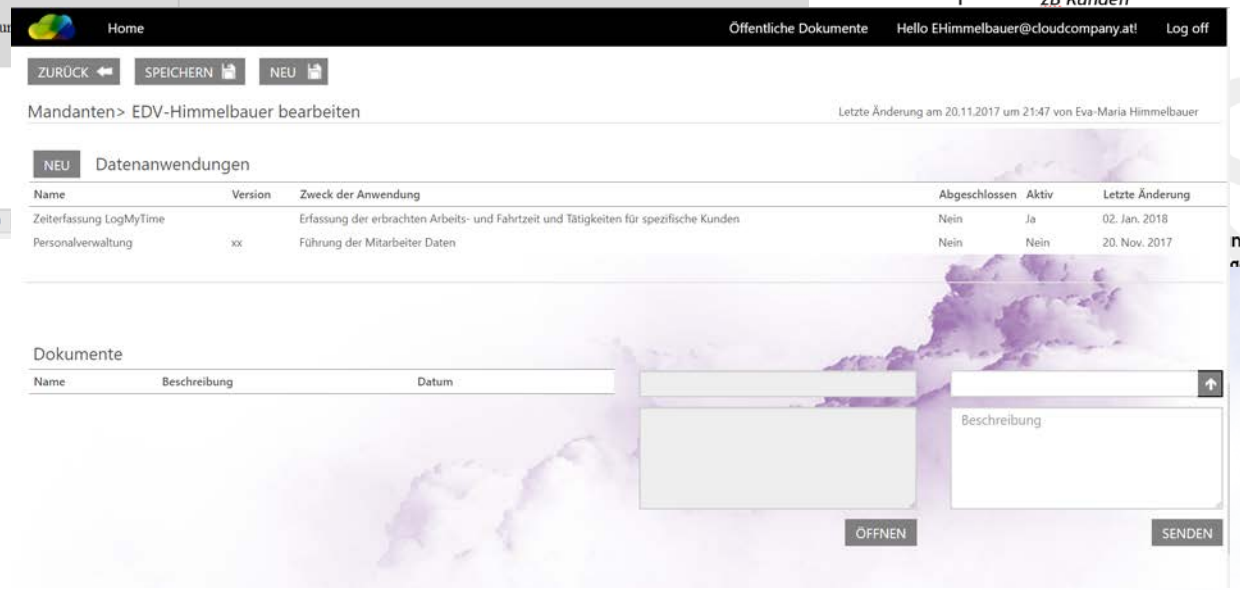
  -> z.B. Banken, Versicherungen, Kreditauskunfteien und Berufsdetektive

- die **Kerntätigkeit** des Unternehmens in der umfangreichen **Verarbeitung sensibler Daten** oder von Daten über strafrechtliche Verurteilungen oder Straftaten besteht

  -> z.B. Krankenanstalten

Verzeichnis über Verarbeitungstätigkeiten





C. Detailangaben zu ..... *(Einfügung der konkreten Datenverarbeitung aus dem B-Blatt, zB des Datenverarbeitungszweckes „Rechnungswesen"; das C-Blatt kann dann für jede der im B-Blatt angegebenen Datenverarbeitungszwecke verwendet werden, ohne dass die allgemeinen Angaben aus dem A- und B-Blatt wiederholt werden müssen)*

1. Kategorien der betroffenen Personen

Lfd.Nr.	*Beschreibung der Kategorien betroffener Personen (zB Kunden, Mitarbeiter, Lieferanten usw.)*
1	*zB Kunden*

ngen oder sonstige Unterlagen (zB Erledigung der

Verzeichnis über Verarbeitungstätigkeiten

Was ist zu erfassen bzw. zu dokumentieren?

- Stammdatenblatt
  - Name des Verantwortlichen
  - Name der Vertreter des Verantwortlichen
  - Kontaktdaten des Verantwortlichen
  - *Name und Kontakt des Datenschutzbeauftragten*

Verzeichnis über Verarbeitungstätigkeiten

Was ist zu erfassen bzw. zu dokumentieren?

- **Name** der Verarbeitung (Prozess)
- Konkreter **Zweck** der Verarbeitung
- Kategorien **betroffener Personen**, deren Daten verarbeitet werden
- **Kategorien personenbezogener Daten**, die verarbeitet werden
- **Kategorien von Empfängern** (tatsächliche, beabsichtigte), denen die personenbezogenen Daten mitgeteilt werden
- **Drittländer**, an die Daten weitergegeben werden, unter Angabe des konkreten Drittlands und bei Ausnahmetransfer die Drittlandsgarantien
- Wenn möglich **Speicherdauer** (+ Grundlage), Fristen für Löschung
- Technischen und organisatorischen Maßnahmen

Beispiele Personalverwaltung

- Personalverwaltung von bestehenden Dienstverhältnissen
- Verwaltung von Bewerbungen bzw Stellenausschreibungen
- Zeiterfassungssysteme
- Zutrittssysteme (Schlüssel- u Chipsysteme)
- Krankmeldungen
- Kündigungen
- An/Abmeldung Krankenkasse
- Personalverrechnung incl Pfändung
- Gehaltszahlungen
- Dienstverträge
- Stellenausschreibungen
- Arbeitsplatzbeschreibungen

Beispiel Rechnungswesen und Geschäftsabwicklung

- Buchhaltung bzw Einnahmen-Ausgaben-Rechnung
- Verarbeitungen im Rahmen des Steuerrechts bzw Übermittlungen an Steuerberater und Finanzamt
- UVAs
- Kostenrechnung
- Verwaltung der Bankkonten bei Kreditinstituten (Zahlungsverkehr)
- Auflagen iZm Registrierkassen
- Ausgangs- und Eingangsrechnungen (Einkauf / Verkauf)
- Miet- und Leasingverträge
- Versicherungen
- Lagerverwaltung (inkl. Inventurunterlagen)
- ….

Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung hat insbesondere dann zu erfolgen, wenn

- **neue Technologien** verwendet werden oder
- **aufgrund der Art, des Umfangs, der Umstände und der Zwecke** der Verarbeitung

voraussichtlich **ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht**.

-> DSB erstellt „Black & White List“

-> Bereits genehmigte DVR Meldungen behalten Gültigkeit

Verträge mit Auftragsverarbeitern

Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

- betrifft Steuerberater, externer Buchhalter, IT Dienstleister, Internetprovider, Cloud Anbieter, Werbeagentur, Postversand, …
- Vereinbarung über Auftragsverarbeitung

  -> Muster Vertrag WKÖ

Verträge mit Auftragsverarbeitern

- Beinhaltet u.a.:
  - Wer ist für die Datenverarbeitung verantwortlich
  - Gegenstand und Dauer der Verarbeitung
  - Art und Zweck der Verarbeitung
  - Art der personenbezogenen Daten und Kategorien von betroffenen Personen
  - Verpflichtung zur Vertraulichkeit
  - Sicherstellung von technischen und organisatorischen Maßnahmen
  - Etwaige Hinzuziehung von Subunternehmern
  - Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsdatenverarbeitung

Verfahrensverzeichnis des Auftragsverarbeiter

- Auftragsverarbeiter führt Verzeichnis über Verarbeitungstätigkeiten je Kunden
- Beinhaltet:
  - Name und Kontaktdaten des Auftragsverarbeiters
  - Name und Kontaktdaten des Verantwortlichen
  - Kategorien von Verarbeitungen
  - ggf Angaben über Übermittlungen von personenbezogenen Daten an ein Drittland oder einer internationalen Organisation
  - allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen

Rechte der Betroffenen

- **Informationspflicht** bei Erhebung von personenbezogenen Daten bei der betroffenen Person
- **Informationspflicht**, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden
- **Auskunftsrecht**
- Recht auf **Berichtigung**
- Recht auf **Löschung** ("Recht auf Vergessenwerden")
- Recht auf **Einschränkung** der Verarbeitung
- Recht auf **Datenübertragbarkeit**
- **Widerspruchsrecht**

Technische & organisatorische Maßnahmen

- **Firewall** zur Abschottung von Zugriffen von Außen
- **VPN** für den Zugriff auf das Firmennetzwerk aus dem Internet
- **Festplattenverschlüsselung** für mobile Geräte (Notebooks)
- **PIN-Code** auf Smartphones
- **Verschlüsselung** von Emails
- **Aktueller Virenschutz**
- Zutritts- und/oder Zugriffskontrolle zu sensiblen analogen Daten (Clean Desk Policy)

Technische & organisatorische Maßnahmen

- Berechtigungsmanagement für den Datenzugriff im Firmennetzwerk
- Password Richtlinien (Komplexität, Änderungen, Verschwiegenheit)
- Blocken von sicherheitsrelevanten Funktionen (z.B. USB-Ports)
- Zugangskontrollen zu sensibler Hardware (zB Server)
- Regelmäßige Datensicherung (Backup- & Recovery Konzept)
- Notfallpläne für IT-Sicherheitsvorfälle

Technische & organisatorische Maßnahmen

- Bindende interne IT- & **Datenschutzrichtlinien**
- Richtlinie zur sicheren Nutzung von IT und Internet
- Social Media Richtlinien
- **Mitarbeiterschulung** (Datenschutz Awareness Training)
- Implementierung von Prozessen zur **regelmäßigen Evaluierung** der Datenschutz- & IT-Sicherheitsrichtlinien

Data Breach Notification

- **Verletzung der Sicherheit**, die, ob unbeabsichtigt oder unrechtmäßig,
  - zur Vernichtung,
  - zum Verlust,
  - zur Veränderung, oder
  - zur unbefugten Offenlegung
  - zum unbefugten Zugang

  zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.
- **Meldung an die zuständige Aufsichtsbehörde**, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt – **innerhalb von 72 Stunden**

Österreichische Datenschutzbehörde
Wickenburggasse 8-10, 1080 Wien
E-Mail: dsb@dsb.gv.at

Data Breach Notification

- **Benachrichtigung der betroffenen Person**, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich **ein hohes Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

Schritte bis zum 25.Mai 2018

- **Status Quo** erfassen
  - Musterverträge, Datenschutzerklärungen, AGBs, Verarbeitungstätigkeiten
  - Rechtsgrundlagen!
  - Löschung?
- *Bestellung Datenschutzbeauftragten?*
- **Verfahrensverzeichnis aufbauen**
- *Risikoanalyse & Folgenabschätzung*
- **Verträge mit Auftragsverarbeitern**
- **Maßnahmen zu Datenschutz und –sicherheit**
  - u.a. Schulung von/Information an Mitarbeitern
  - Überprüfung der IT Sicherheit (Firewall, Anti-Viren Schutz, Passwörter, Back-Ups, …)
- **Laufende Kontrolle**

Unterstützung DSGVO Umsetzung

- KMU Digital Förderung u.a. betreffend Verbesserung der IT-Sicherheit und des Datenschutzes
- 50% für Beratung und Qualifizierung
- Bis zu 4.000 Euro Förderung für Ihr Unternehmen!
- Infos unter www.kmu-digital.at

Danke!

Alle Infos unter www.cloudcompany.at/WBDSGVO