Datenschutzgrundverordnung DSGVO

Ab dem 25.5.2018 gelten die EU-Datenschutz-Grundverordnung (DSGVO) und das österreichische Datenschutzgesetz (DSG) in der Fassung des Datenschutz-Anpassungsgesetz 2018. Das bedeutet für alle Unternehmen zum einen Handlungsbedarf bei Verträgen, internen Abläufen sowie Datensicherheitsmaßnahmen und zum anderen verschärfte Strafdrohungen.

Jede Firma welche mit personenbezogenen Daten arbeitet, sollte sich folgende Fragen stellen:

- Um wessen Daten geht es?
    - Mitarbeiter
    - Kunden
    - Lieferanten
    - Kooprationspartner
- 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
    - 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!**
- Was ist Datenverarbeitung?
  Verarbeitung als weitgefasster Begriff
    - Erheben / Erfassen
    - Speicherung
    - Verwendung
    - Weitergabe / Verbreitung
    - Löschen / Vernichtung etc

→ z.B. Erstellung einer Kundendatei, Datenaufnahme zur Erstellung einer Rechnung, Mitarbeiterdatenbank

- Verarbeitung im Rahmen der Tätigkeit einer Niederlassung in der EU
- Verarbeitung findet überall statt (z.B. Cloud)
- Automatisierte Verarbeitung
    - Maschinell und programmgesteuert
    - Verarbeitung nicht ausschließlich vom Menschen alleine
- Teilweise automatisierte Verarbeitung
    - Einige Verarbeitungsschritte manuell + einige Verarbeitungsschritte automatisiert
    - B. Verfassen eines E-Mails, Verfassen eines Kündigungsschreibens im Word, Kundenverzeichnis als Excel-Datei
- Nichtautomatisierte / manuelle Verarbeitung
    - Daten sind oder sollen in Dateisystem gesammelt werden
    - Dateisystem = strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind
      B. (Papier-)Akte, Karteien, Karteikästen, Datenbank
    - B. handschriftliche Aufzeichnungen werden in Karteisystem abgelegt oder in automationsunterstützten Datenbank gespeichert
- Persönliches Wissen?
    - Verarbeitbarkeit von Informationen erfordert Fixierung in verarbeitbarer Form
      Mangels Fixierung → **DSG-VO nicht anwendbar**
- Mit welchen Sanktionen habe ich im Fall unzulässiger Datenverarbeitung zu rechnen?
    - 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