Grundlagen «Datenschutz»

Hier haben wir euch/Ihnen die wichtigsten Begriffe im Zusammenhang mit dem revDSG kurz erklärt:

Wichtigste Neuerungen:

- Generelle Transparenzpflicht (auch Mitarbeiter informieren)
- Bussen bei Verletzung von Informations-, Auskunfts- und Sorgfaltspflicht (Bussen von CHF 10'000 bis 250'000)
- Strengere Regeln zum Ausland-Transfer von Personendaten (Liste der erlaubten Länder sind Teil des revDSG)
- Dokumentationspflichten, insbesondere bei risikoreichen Vorhaben (insbesondere Datenbearbeitunstätigkeit)

Was sind Personendaten?

Personendaten sind Informationen über identifizierte oder identifizierbare natürliche Personen (Einzelfirmen sind auch «natürliche Personen»)

Welches sind schützenswerte Daten?

- Daten über die Gesundheit oder die Intimsphäre
- Daten über die Zugehörigkeit zu einer Rasse oder Ethnie
- Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten und Tätigkeiten
- Genetische Daten
- Biometrische Daten, die eine Person eindeutig identifizieren
- Daten über die Massnahmen der sozialen Hilfe
- Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen

Merke: bei den meisten KMU fallen solche Daten im HR-Bereich an (Krankheit, Unfälle, Strafregisterauszüge bei Bewerbungen, Abrechnung mit Gewerkschaft für Parifond, Konfession, etc.)

Bearbeiten heisst...

Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten der Daten (diese Aufzählung ist nicht abschliessend)

Datenbearbeitungen sind immer zulässig, solange die Grundsätze erfüllt sind

Wenn ein Rechtfertigungsgrundsatz vorliegt, ist die Datenbearbeitung auch zulässig, wenn sie gegen die Bearbeitungsgrundsätze verstösst.

Bearbeitungsgrundsätze:

- *Rechtsmässigkeit und Treu und Glauben* = es dürfen nur Daten bearbeitet werden, die nicht illegal erworben wurden und keine schützenswerte Personendaten an unerlaubte Dritte bekannt gegeben werden (bei rechtlicher Grundlage, wie z.Bsp. AHV ist die Weitergabe von Gesetzes wegen rechtmässig).

- *Transparenz und Zweckgebundenheit* = Informieren Sie in der Datenschutzerklärung klar und offen darüber, welche Personendaten Sie erheben und für welche Zwecke Sie diese bearbeiten und halten Sie sich daran. Der Zweck kann sich auch aus den Umständen oder gesetzlichen Vorgaben ergeben.

- *Verhältnismässigkeit* = nur Daten erheben und bearbeiten, die geeignet und erforderlich sind, um den verfolgten Zweck zu erreichen (Datensparsamkeit).
  Daten zu löschen oder zu anonymisieren, wenn sie nicht mehr benötigt werden und keine Aufbewahrungspflicht mehr besteht.
  Innerhalb der Unternehmung die Mitarbeiter nur auf jene Daten Zugriff erhalten, welche sie zur Erfüllung ihrer Arbeit zwingend benötigen.

- *"Privacy by Design" und "Privacy by Default"* =
  «Privacy by Design» Ausgestaltung von Prozessen bzw. Software oder Hardware zur Datenverarbeitung nach dem Prinzip «Datenschutz durch Technikgestaltung». Dies umfasst beispielsweise die Nutzung von Verschlüsselungstechniken und die zurückhaltende Erfassung und Speicherung von Daten.
  «Privacy by Default» Ausgestaltung von Prozessen nach dem Prinzip «datenschutzfreundliche Voreinstellungen».
  Diese datenschutzfreundlichen Voreinstellungen sind in der sogenannten «User Experience» zu beachten.

- *Datenrichtigkeit* = Unrichtige oder unvollständige Personendaten müssen berichtigt und ergänzt werden. Geht dies nicht sind die Daten im Zweifel zu löschen. Die betroffene Person kann jederzeit eine Korrektur der eigenen Daten verlangen.

Rechfertigungsgrundsatz:

- Einwilligung durch die betroffene Person (empfohlen schriftlich oder durch digitale Einwilligung, aber grundsätzlich formfrei möglich) = kann jederzeit widerrufen werden
- Datenbearbeitung infolge einer gesetzlichen Vorgabe
- Überwiegendes privates oder öffentliches Interesse (Bsp. Datenbearbeitung zur Prüfung der Kreditwürdigkeit, Datenbearbeitung im Zusammenhang mit Vertragsabschluss, weitere in Artikel 31 DSG)

Ich trage die Verantwortung für eine gesetzeskonforme Datenbearbeitung!

- Einhaltung der Bearbeitungsgrundsätze
- Einholen der ausdrücklichen Einwilligung bei besonders schützenswerten Daten (Gesundheitsdaten, Biometrische Daten, etc.)
- Sorgfältige Auswahl von Auftragsbearbeitern (Homepagbetreiber, IT-ler, Treuhänder, etc.) →Auftragsdatenbearbeitungsvertrag (ADV)
- Führung eines Datenverarbeitungs-/Datenbearbeitungsverzeichnisses empfohlen (bei + 250+ und Risikoreichen Daten oblig.)
- Ergreifen von technischen und organisatorischen Massnahmen
- Informationspflicht gegenüber betroffenen Personen
- Pflichten im Zusammenhang mit den Rechten der betroffenen Personen (Auskunftspflicht, Pflicht zur Löschung/Berichtigung/Herausgabe von Daten)
- Meldepflicht an EDÖB (Data Breach Notification)
- Ev. Erstellung einer Datenschutz-Folgeabschätzung
- Datenschutzerklärung erstellen und allfällig anpassen

Informationspflicht

Die Informationspflicht wird über die **Datenschutzerklärung** erfüllt, diese ist ebenfalls Teil des Bearbeitungsgrundsatz Transparenz

- Über die Beschaffung von Personendaten (auch, wenn Daten bei Dritten beschafft werden).
- Informationen, die für die Betroffenen notwendig sind, um Rechte nach dem revDSG geltend zu machen.
- Mindestinhalte:
    - Indentität und Kontaktdaten des Verantwortlichen
    - Bearbeitungszweck
    - Kategorien von Empfänger von Personendaten
    - Bekanntgabe ins Ausland
- Risikobasierter Ansatz: Je heikler Datenbearbeitung, umso genauer und umfangreicher die Information.
- Form: Die Datenschutzerklärung untersteht keiner Formvorschrift (jedoch einfach auffindbar auf der Webseite)

→ Die **Liste der Staaten mit einem angemessenen Datenschutzniveau** wird vom Bundesrat beschlossen und ist unter https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html#-2053327153 abrufbar.

Datensicherheit

Welche Schutzziele müssen erreicht werden?

- **Vertraulichkeit**
- **Verfügbarkeit**
- **Integrität**
- **Nachvollziehbarkeit**

Grundsatz: Jedes Unternehmen muss durch technische und organisatorische Massnahmen eine angemessene Datensicherheit gewährleisten.

Datensicherheit: Daten absichern gegen Manipulation, Verlust, Diebstahl/Einsicht

Datenschutz-Folgeabschätzung

- Instrument zur Erkennung von Datenschutzrisiken bei bestimmten Datenbearbeitungen, zu deren Bewertung und Definition von Massnahmen.
- Notwendig bei hohem Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen
- Ein hohes Risiko liegt vor:
    - bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten
    - wenn systematisch umfangreiche öffentliche Bereiche überwacht werden

→ Ergibt sich auch aus der DSFA immer noch ein hohes Risiko, muss vor der Aufnahme der geplanten Datenbearbeitung die **Stellungnahme des EDÖB eingeholt** werden.

Auftragsdatenbearbeitung

Bei jeder Auslagerung von Datenbearbeitungen muss Folgendes beachtet werden:

- Erfüllt der Auftragsbearbeiter die notwendigen Sicherheitsstandarts?
- Wurde ein Auftragsdatenbearbeitungsvertrag ("ADV") abgeschlossen?
- Erfüllt der Auftragsbearbeiter die Anforderungen betreffend der technischen und organisatorischen Massnahmen zur Datensicherheit?
- Welche Subunternehmer zieht der Auftragsbearbeiter bei und sind diese auf dem ADV aufgeführt?
- Kann der Auftragsbearbeiter Datenverluste und Beschädigungen feststellen und Sie umgehend informieren?

Meldepflicht

- Bei einer Datensicherheitsverletzung besteht eine Meldepflicht gegenüber dem EDÖB, wenn dies voraussichtlich zu einem Risiko für die betroffenen Personen führt.
- Zudem muss eine Meldung gegenüber den Betroffenen erfolgen, wenn dies für deren Schutz notwendig ist (Beispiel: Passwortschutz)
- Inhalt der Meldung:
    - Art der Verletzung der Datensicherheit
    - Folgen
    - die ergriffenen oder vorgesehenen Massnahmen

Nützliche Tools und Links

- Verständliche Erklärung für jeden eingesetzten Dienst auf der Webseite
  Link Privacy Bee
  ab CHF 4.00 / pro Monat
  Version mit eigenen Felder kommt im Herbst
  Integration auf Homepage durch comvation

- Archiv+ Revisionssichere Ablage- und Archivierungssystem (MWS Dinotronic und SwiDoc Archivplattform), zertifiziert gemäss GebüV
  swiss digital future by b managed
  ab CHF 99.00 / Monat
  Beratung durch zertifizierte Datenschutzberaterin: Cornelia Boss

- Sensibilisierung zu Cybersicherheit
  Link S-U-P-E-R
  Sichern – Updaten – Prüfen – Einloggen – Reduzieren

Zusammenfassung

Das revidierte Datenschutzgesetz tritt am 01. September 2023 in Kraft. Die Übergangsfrist wurde mit der frühzeitigen Bereitstellung von Gesetz und Verordnung faktisch bereits gewährt.

- Gehen Sie die Umsetzung des revidierten Datenschutzgesetzes in ihrer Organisation mit einem Plan an.
- Denken Sie an die Sensibilisierung Ihrer Mitarbeitenden als Führungsaufgabe - dies laufend mit verschiedenen Aktivitäten.
  - Datenschutz und Informationssicherheit in Meetings thematisieren.
  - Bereitstellung von Checklisten.
- Definieren Sie interne Kontrollen (z. B. für Zugriffsrecht-Kontrollen, Kontrolle der Verzeichnisse der Bearbeitungstätigkeiten, Kontrolle der Auftragsdatenbearbeitungen) durch.
- Informieren Sie über die Ergebnisse der Kontrollen angemessen und transparent in internen Meetings oder bei Bedarf in persönlichen Gesprächen.

Wir leben und arbeiten in einer zunehmend digitalen Welt – tragen wir zur Sicherheit bei. Darum sind Datenschutz und Informationssicherheit, Führungsaufgaben und nicht nur das Thema von «Geeks» oder «Freaks».