# EU-DSGVO
# Datenschutz-Compliance

27. März 2018

Stefano Caldoro

# Inhaltsübersicht



1. Einführung
2. Was betrifft es?
3. Auch für Schweizer Unternehmen relevant?
4. Anforderungen der DSGVO, die Sie kennen müssen
5. Rechtsfolgen bei Verstössen
6. Handlungsbedarf

3

# Einführung

- Wann?
- Ziele
- Scharfe Anforderungen

# Es geht los



# 25. Mai 2018

# Ziele



1. Datenschutz als Grundrecht
   - Schutz natürlicher Personen (u.a. wegen technischer Entwicklung)
   - Ausgewogenheit wirtschaftliche Interessen - Konsumentenschutz
2. "Lex Irland"
   - Harmonisierung (gleiches Datenschutzniveau) und Kohärenzverfahren (gleiche Auslegung und Anwendung)
   - Unmittelbare Anwendung
3. "Lex USA"
   - Forderung nach Datenschutzniveau
4. "Lex Facebook etc."
   - Digitalisierungsgefahren (Datenübertragbarkeit, Profiling, Transparenz)

# Scharfe Anforderungen



- Verbotsgesetz mir Erlaubnisvorbehalt
- Weitreichende Rechte der Betroffenen und höhere Anforderungen an Einwilligung
- Erweiterte Transparenzpflichten der Unternehmen (inkl. Info- und Meldepflichten)
- Nachverfolgbarkeit der Verarbeitung der Daten (z.B. welche Daten, wie verarbeitet, woher, wo gespeichert, wie analysiert)
- Prozesse und Richtlinien zur Risikovorbeugung und zur Einhaltung der Grundsätze
- Prozesse und Richtlinien zu Reaktionsmassnahmen
- Dokumentationspflichten
- Hohe Sanktionen

☞ Umsetzung eines betrieblichen Datenschutz-Management Systems!

# Was betrifft es?

- Personendaten
- Verarbeitung
- Verantwortlicher und Auftragsverarbeiter

# Personendaten



- Informationen, die sich auf identifizierte oder identifizierbare Person beziehen
- "Identifizierbar": wenn Betroffener direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung identifiziert werden kann

  *Bsp. Namen, Adresse, Telefonnummer, Kennnummer (z.B. Autokennzeichen, Bankdaten), Standortdaten, Online-Kennung wie IP-Adressen und Cookie-Kennungen*

- Keine Anwendung der EU-DSGVO auf anonyme oder anonymisierte Informationen und auf Daten Verstorbener
- Sensible Daten (besondere Kategorien): Daten, aus denen rassische/ethnische Herkunft, politische Meinungen, religiöse/weltanschauliche Überzeugungen hervorgehen; genetischen Daten; biometrischen Daten; Gesundheitsdaten; Daten zur sexuellen Orientierung

  *Bsp. Fingerabdruck, Iriscan, Krankengeschickte*

# Verarbeitung



- Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang im Zusammenhang mit Personendaten wie Erheben, Erfassen, Speichern, Verwenden, Ändern, Auslesen, Abfragen, Übermitteln, Einschränken, Löschen, Vernichten usw.

  *Bsp. Erstellung Kundendatei, Datenaufnahme zur Rechnungserstellung, Mitarbeiterdatenbank*

- DSGVO anwendbar auf:

  a) Die ganz oder teilweise automatisierte Verarbeitung (z.B. mit Computer, Internet, E-Mail, Smartphones, Kameras, Webcams, Scanner, Kopierer) und

  b) die nichtautomatisierte (z.B. handschriftliche) Verarbeitung von Daten, die in einem Dateisystem (d.h. strukturierter Sammlung von Daten, die nach bestimmten Kriterien zugänglich sind) gespeichert bzw. zu speichern sind.

# Beispiele relevanter Tätigkeiten



Kundendatenauswertungen

Direktwerbemassnahmen

Tracking von Website-Besuchern

Profiling
(jede automatisierte Bearbeitung von Daten, die dazu verwendet werden, bestimmte persönliche Aspekte einer Person zu bewerten, analysieren oder vorherzusagen, z.B. bezüglich Arbeitsleistung, Gesundheit, wirtschaftliche Lage, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel).

Bsp. *Automationsunterstützte Analyse der Kreditwürdigkeit eines Kunden*

Datenübermittlung ins Ausland

Auftragsdatenbearbeitung, z.B.

- Auslagerung von Kundenbewirtschaftung, Lohnbuchhaltung usw.
- Kundenbefragung / -datenauswertung
- Übertragung Zahlungsunfähigkeitsrisiko u. Debitorenumtriebe an Factoring-Firma
- IT-Outsourcing, Cloud-Computing, Hosting, IT-Backup, IT-Archivierung
- Tracking, Profiling, Data Mining
- kollektive Taggeldversicherung

Human Resources-Aktivitäten, z.B.

- Bearbeitung des Personaldossiers
- Personensicherheitsprüfung
- Überwachung am Arbeitsplatz
- Zugriff auf E-Mails der Angestellten

# Verantwortlicher / Autragsverarbeiter



- **Verantwortlicher**: Wer über die Zwecke und Mittel der Verarbeitung von Personendaten entscheidet.

- **Auftragsverarbeiter**: Wer Personendaten im Auftrag des Verantwortlichen bearbeitet.

  *Bsp.: Der externe Buchhalter, der die Daten für die Bilanzerstellung vom Unternehmer erhält und bearbeitet; Rechenzentrum; Cloud-Anbieter; usw.*

  Der Auftragsverarbeiter hat unmittelbare Pflichten (z.B. Führung eines Verzeichnisses der für den Datenverantwortlichen durchgeführten Bearbeitungstätigkeiten, unverzügliche Meldung von Datenschutzverstössen)

# Autragsverarbeiter



- Sorgfältige Auswahl: Verarbeiter muss die DSGVO-konforme Verarbeitung durch die Umsetzung von technischen u. organisatorischen Massnahmen sicherstellen können.

- Schriftlicher Vertrag – Zwingender Inhalt:
  - Gegenstand, Zweck und Dauer der Verarbeitung
  - Art der personenbezogenen Daten
  - Kategorien betroffener Personen
  - Pflichten des Auftragsverarbeiters:
    - Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen
    - Vertraulichkeit
    - Ergreifen von Datensicherheitsmassnahmen
    - Keine Unterbeauftragung ohne vorherige schriftliche Genehmigung d. Verantwortlichen
    - Unterstützungspflicht
    - Dokumentationspflicht

# Auch für Schweizer Unternehmen?

# Anwendung auf



I. Unternehmen mit Niederlassung in der EU, selbst wenn die Verarbeitung der Daten für dieses Unternehmen gar nicht in der EU stattfindet (Niederlassungsprinzip)

*Bsp.: Die deutsche Tochtergesellschaft eines CH-Unternehmens bearbeitet Kundendaten und speichert sie in den USA.*

II. Unternehmen, die im Einzelfall durch Rechtswahl die Anwendung des Rechts eines EU-Mitgliedstaates vereinbaren.

# Anwendung auf



III. Unternehmen, die innerhalb der EU Geschäfte machen (Marktordnungsprinzip):

1. CH-Unternehmen, das Daten von Personen in der EU bearbeitet, um diesen *Waren oder Dienstleistungen (entgeltlich oder unentgeltlich) anzubieten*

   *Bsp.: Brauerei, die Produkte an Interessenten in der EU aufgrund einer Liste von E-Mail-Adressen anbietet; Website in der Schweiz, die Liefer- und Zahlungskonditionen für Ausländer erwähnt; CH-Unternehmen mit Service-Hotline in EU.*

2. CH-Unternehmen, das Daten von Personen in der EU bearbeitet, um das *Verhalten dieser Personen zu beobachten*, soweit ihr Verhalten in der EU erfolgt

   *Bsp.: Datenanalyse von Besuchern einer Webseite oder Nutzern einer App zu Marketingzwecken, wie mit Tracking durch Cookies; Profiling durch Analysetools.*

3. CH-Unternehmen, das an der Datenbearbeitung *als Auftragsverarbeiter mitwirkt*

   *Bsp.: Unternehmen, das in der Schweiz Daten für Tochtergesellschaft in der EU bearbeitet; Schweizer Rechenzentren, die für Unternehmen in der EU tätig sind.*

# Anforderungen, die man kennen muss

1. Bearbeitungsgrundsätze
2. Rechtfertigungsgrund, Einwilligung
3. Informationspflicht, Betroffenenrechte
4. Technische und organisatorische Massnahmen
5. Datenschutz-Folgeabschätzung
6. Accountability
7. Meldungen von Datenschutzverletzungen
8. Datenübermittlung ins Ausland
9. Datenschutzbeauftragter und Datenschutzvertreter

# Bearbeitungsgrundsätze



- Rechtmässigkeit, Treu und Glauben
- Transparenz – alle Informationen zur Verarbeitung leicht zugänglich und verständlich in klarer und einfacher Sprache abgefasst
- Zweckbindung – Erhebung und Verwendung nur für festgelegte, eindeutige und legitime Zwecke
- Verhältnismässigkeit (Datenminimierung) – auf das für den Verarbeitungszweck notwendige Mass beschränkt
- Richtigkeit der Daten
- Speicherbegrenzung (nur so lange, wie für die Verarbeitungszwecke erforderlich)
- Datensicherheit
- Rechenschaftspflicht (für Einhaltung und Nachweis der Einhaltung)

# Anforderungen, die man kennen muss

1. Bearbeitungsgrundsätze
2. Rechtfertigungsgrund, Einwilligung
3. Informationspflicht, Betroffenenrechte
4. Technische und organisatorische Massnahmen
5. Datenschutz-Folgeabschätzung
6. Accountability
7. Meldungen von Datenschutzverletzungen
8. Datenübermittlung ins Ausland
9. Datenschutzbeauftragter und Datenschutzvertreter

# Rechtfertigungsgrund



1. Einwilligung

   *Bsp. Besucher einer Website willigt ausdrücklich ein, vom Unternehmen Newsletter zu erhalten.*

2. Zur Erfüllung eines Vertrags erforderlich (Betroffener als Partei)

   *Bsp. Die Adresse des Käufers wird gespeichert und verarbeitet für die Bestellung, Lieferung und Zahlungsabwicklung.*

3. Zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen erforderlich

   *Bsp. Verarbeitung von Daten des Mitarbeiters zur Einhaltung arbeitsrechtlicher Pflichten.*

4. Zum Schutz lebenswichtiger Interessen des Betroffenen oder Dritten erforderlich

5. Für die Wahrnehmung einer Aufgabe im öffentlichen Interesse erforderlich

# Rechtfertigungsgrund



6. Zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen des Betroffenen Person überwiegen
   → Interessenabwägung im Einzelfall

   Mit welchen Bearbeitungen muss der Betroffene im Zeitpunkt der Datenbeschaffung aufgrund der Umstände rechnen?

   Nach DGSVO kann auch Direktwerbung als berechtigtes Interesse betrachtet werden

   *Bsp. Zusendung von Werbematerial an einen bestehenden Kunden per Post (per E-Mail ist in der Regel vorherige Einwilligung notwendig) könnte als berechtigtes Interesse gesehen werden.*

   In Zweifelsfällen wird aber in der Praxis auch im Bereich des "berechtigten Interesses" oft mit einer Einwilligung (z.B. via Checkbox) gearbeitet werden müssen.

# Rechtfertigungsgrund



**Verarbeitung von sensiblen Daten** ist grundsätzlich untersagt. Ausnahmen:

- ausdrückliche Einwilligung oder
- andere besonderen gesetzlich vorgesehenen Gründe (z.B. Ausübung von Rechten aus Arbeitsrecht, sozialer Sicherheit und Sozialschutz; zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen; lebenswichtige Interesse des Betroffenen, der ausserstande ist, die Einwilligung zu geben; erhebliche öffentliche Interessen)

☞ *Zunächst prüfen, welche Daten zu welchen Zwecken wie lange verarbeitet werden und ob bereits eine andere Rechtsgrundlage vorliegt. Je nachdem ist keine Einwilligung notwendig.*

# Rechtfertigungsgrund



Eine **Weiterverarbeitung** ist für einen anderen Zweck nur dann zulässig:

- Einwilligung oder
- Gesetzliche Grundlage oder
- Vereinbarkeit mit den Zwecken, für welche die Daten ursprünglich erhoben wurden. (zu beurteilende Faktoren: Verbindung zwischen altem und neuem Zweck; Zusammenhang, in dem die Daten erhoben wurden; Art der Daten; mögliche Folgen der Weiterverarbeitung für den Betroffenen; Vorhandensein angemessener Garantien wie Pseudonymisierung) und Information des Betroffenen über den neuen Zweck vor dieser Weiterverarbeitung

*Bsp. Kundendaten, die für eine Vertragsabwicklung erhoben wurden (z.B. Geburtstagsdatum) zur Altersüberprüfung, sollen für Marketingzwecke verwendet werden (z.B. Geburtstagskarte). Das kann zulässig sein, wenn der Betroffene im Voraus (z.B. in der Datenschutzerklärung) informiert wird und Vertraulichkeit gewährleistet wird (z.B. keine offene Postkarte).*

# Einwilligung



- Formfrei (auch konkludent, durch Anklicken eines Kästchens auf einer Internetseite) – NICHT aber bereits vorangekreuzte Kästchen

  Ausdrücklich bei sensiblen Daten

- Freiwillig:

  a) Bei mehrerer Zwecken: Gesonderte Einwilligung für jeden Zweck

     *Bsp.: Erhebung Daten durch Reiseveranstalter für Buchung und Übermittlung an Hotel.*

  b) Koppelungsverbot

     *Bsp.: Dienstleistung wird von der Einwilligung zur Datenbearbeitung abhängig gemacht, die für die Erbringung der Dienstleistung nicht erforderlich ist (z.B. bei Gewinnspielen, Anmeldungen für Events, Download von Dokumenten usw.).*

  c) Kein erhebliches Ungleichgewicht Verantwortlicher-Betroffener

- Für den bestimmten Fall, in informierter Weise (detaillierte Information im Voraus)

# Einwilligung



- Unmissverständlich
  - Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache
  - Einwilligungserklärung von anderen Sachverhalten (z.B. in AGB) klar getrennt dargestellt (z.B. Separierung in anderem Text oder optische Hervorhebung)
- Beweislast des Verantwortlichen
- Jederzeit widerrufbar (Betroffene ist darauf im Voraus hinzuweisen)
- Jugendliche unter 16 Jahren: Zustimmung der Eltern

☞ *Bemerkung: Alte Einwilligungen gelten nur weiter, wenn sie die Anforderungen der DSGVO einhalten.*

# Einwilligung: Beispiel Newsletter



- Newsletter-Anmeldeformular auf der Webseite (z.B. Registrierungsmaske mit Eingabe von Namen und E-Mail-Adresse)
- mit kurzem Hinweistext, der den Nutzer aufklärt, was mit den Daten passiert, und mit einem Link zur Datenschutzerklärung.

  *z.B. "Ihre E-Mail-Adresse wird an den Newsletter-Dienstleister XY zum technischen Versand weitergegeben. Weitere Informationen finden Sie in unserer Datenschutzerklärung [Link]."*
- Datenschutzerklärung: Hinweis auf Einwilligung mit Registrierung; Protokollierung der Anmeldungen zum Nachweis des Anmeldeprozesses: Name, E-Mail-Adresse, Datum, Uhrzeit.
- Protokollierung zum Nachweis (auch der Änderungen).
- Insbesondere im Fall eines Online-Shops muss das Newsletter-Anmeldeformular von den Bestellungsfunktionen gut getrennt sein (Koppelungsverbot) und nicht bereits im Vorfeld aktiv/angekreuzt sein (aktive Einwilligung).

# Anforderungen, die man kennen muss

1. Bearbeitungsgrundsätze
2. Rechtfertigungsgrund, Einwilligung
3. Informationspflicht, Betroffenenrechte
4. Technische und organisatorische Massnahmen
5. Datenschutz-Folgeabschätzung
6. Accountability
7. Meldungen von Datenschutzverletzungen
8. Datenübermittlung ins Ausland
9. Datenschutzbeauftragter und Datenschutzvertreter

# Umfassende Information



- Umfassende und aktive Pflicht des Verantwortlichen (immer)
- *Zeitpunkt*: bereits beim Erstkontakt (oder innert Monatsfrist nach Erlangung der Personendaten aus Drittquellen)
- *Umfassenden Mindestinhalt*:
  - Namen und Kontaktdaten des Verantwortlichen, Datenschutzvertreters und -beauftragen
  - Zweck und Rechtsgrundlage, berechtigte Interessen (evtl.), gesetzliche Pflicht (evtl.)
  - Datenkategorien
  - Empfänger und Empfängerkategorien
  - Absicht der Übermittlung ins Ausland (inkl. Angemessenheitsgrundlage oder Garantien)
  - Dauer der Speicherung oder Kriterien zu deren Festlegung
  - Rechte der Betroffenen
  - Bestehen automatisierter Einzelfallentscheide (inkl. Profiling) mit entsprechenden Kriterien

# Umfassende Information



- Präzise, transparente, verständliche, leicht zugängliche *Form*; klare, einfache *Sprache*

  im konkreten Einzelfall oder mindestens allgemein vorab in Datenschutzerklärungen oder in AGB über gut sichtbaren und verständlichen Link.

- Auch bei indirekter Datenbeschaffung oder jeder Änderung des Bearbeitungszwecks

- Ausnahmen:
  - Betroffene verfügt bereits über die Informationen
  - Erteilung dieser Informationen würde die Verwirklichung der Ziele der Verarbeitung unmöglich machen oder ernsthaft beeinträchtigen
  - Personendaten unterliegen einem Berufsgeheimnis oder Geheimhaltungspflicht

# Betroffenenrechte



- Auskunft
- Berichtigung
- Löschung
- Beschränkung
- Weitermeldung von Berichtigung, Löschung und Beschränkung
- Datenportabilität
- Widerspruch
- Widerruf der Einwilligung
- Beschwerde bei der Aufsichtsbehörde
- Anhörung bei automatisierten Einzelfallentscheiden

# Betroffenenrechte



## Auskunft

- über alle Details der Bearbeitung (Kopien der Daten, Zwecke, Kategorien, Empfänger, Dauer, Überlieferung ins Ausland, Rechte des Betroffenen, Regelungen betr. automatisierte Generierung von Einzelentscheidungen (inkl. Profiling) sowie
- über alle aufgrund der Datenbearbeitung gefällten Entscheidungen
- evtl. Negativauskunft (keine Daten vorliegend)
- Kein Eingriff in Rechte Dritter (z.B. Schwärzung Daten Dritter)

## Berichtigung

- Falsche Daten (z.B. falsches Geburtsdatum) oder unvollständige Daten für den Verarbeitungszweck

# Betroffenenrechte



**Unverzügliche Löschung,** wenn

- Daten für die ursprünglichen Verarbeitungszwecke nicht mehr notwendig sind
- Betroffener seine Einwilligung widerrufen hat
- Betroffener Widerspruch gegen die Verarbeitung eingelegt hat
- Daten unrechtmässig verarbeitet werden
- Löschung für die Erfüllung einer gesetzlichen Frist erforderlich ist

**Beschränkung**, wenn

- Betroffener die Richtigkeit der personenbezogenen Daten bestreitet
- Verarbeitung unrechtmässig ist, der Betroffene aber keine Löschung will
- Verantwortlicher die Daten nicht länger benötigt hat, Betroffener aber die Weiterspeicherung zur Geltendmachung von Rechtsansprüchen braucht
- Betroffener Widerspruch gegen die Verarbeitung eingelegt

# Betroffenenrechte



**Weitermeldung** des Begehrens auf Löschung/Berichtigung/Beschränkung

- Angemessene Massnahmen, um andere Verantwortliche zu informieren (Löschung aller Links zu Personendaten und Herausgabe aller Kopien)
- Ausnahme nur, wenn Mitteilung unmöglich oder unverhältnismässig aufwendig

**Widerspruch** gegen bestimme Verarbeitungsarten, z.B. Verarbeitung

- zu Direktmarketing-Zwecken
- zur Wahrnehmung Aufgabe im öffentlichen Interesse; zur Wahrung berechtigter Interessen des Verantwortlichen/Dritten; zu statistischen u.a. Zwecken – solange *der Betroffene Gründe vorbringt, die sich aus seiner besonderen Situation ergeben*

**Datenportatbilität** (Herausgabe oder Übertragung an einen Nachfolger in einem gängigen maschinenlesbaren Format)

# Betroffenenrechte



- Formlose Anträge
- Gegenüber dem Verantwortlichen (Auftragsbeauftragter muss Anfrage weiterleiten)
- Antwort des Verantwortlichen grundsätzlich schriftlich
- Unentgeltliche Anträge (ausser wenn exzessiv oder offenkundig unbegründet)
- Ablehnungsrecht des Verantwortlichen

  (a) Wenn exzessiv oder offenkundig unbegründet (Beweislast bei Verantwortlichen)

  (b) hinzu bei Löschungsrecht: (i) zur Ausübung der Meinungsäusserungsfreiheit, (ii) zur Erfüllung einer gesetzlichen Pflicht, (iii) aus Gründen des öffentlichen Interesses (Gesundheit, wissenschaftliche, historische, statistische Zwecke), (iv) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

# Betroffenenrechte



- Frist zu erfüllen:
  - Auskunft: Innert Monatsfrist (wenn komplex, um 2 Monate verlängerbar)
  - Löschung, Berichtigung, Beschränkung, Widerspruch: unverzüglich, d.h. wenn Antrag innerhalb einer nach Umständen des Einzelfalles zu bemessenden Prüfungs- und Überlegungszeit erledigt wird.

    Wenn Berichtigung/Löschung nicht möglich unverzüglich (aus wirtschaftlichen oder technischen Gründen) → Aufschiebung bis zum erstmöglichen Zeitpunkt.

    Grundsätzlich Maximalfrist von 1 Monat (um 2 verlängerbar)
  - Antwort innert Monatsfrist auch bei

    a) Fristverlängerung um 2 Monate mit Begründung

    b) Nicht-Tätigwerden mit Begründung und Hinweis auf Beschwerderecht

# Anforderungen, die man kennen muss

1. Bearbeitungsgrundsätze
2. Rechtfertigungsgrund, Einwilligung
3. Informationspflicht, Betroffenenrechte
4. Technische und organisatorische Massnahmen
5. Datenschutz-Folgeabschätzung
6. Accountability
7. Meldungen von Datenschutzverletzungen
8. Datenübermittlung ins Ausland
9. Datenschutzbeauftragter und Datenschutzvertreter

# Technische und organisatorische Massnahmen



- Privacy by Design – Datenbearbeitungssysteme müssen *von Anfang an (ab Planung)* datenschutzfreundlich ausgestaltet, z.B. durch
  - Datenminimierung
  - Pseudonymisierung
  - Sicherstellung der Systeme
  - Wiederherstellungsfähigkeit
  - Transparente Datenverarbeitungsprozesse
  - Funktionen, die es dem Nutzer selbst erlauben, die Verarbeitung zu überwachen
  - Mechanismen für den unentgeltlichen Zugang des Betroffenen zu seinen Daten
- Privacy by Default – Datenschutzfreundliche Voreinstellung
- Massnahmen regelmässig nach risikobasiertem Ansatz überprüfen und anpassen.

# Anforderungen, die man kennen muss

1. Bearbeitungsgrundsätze
2. Rechtfertigungsgrund, Einwilligung
3. Informationspflicht, Betroffenenrechte
4. Technische und organisatorische Massnahmen
5. Datenschutz-Folgeabschätzung
6. Accountability
7. Meldungen von Datenschutzverletzungen
8. Datenübermittlung ins Ausland
9. Datenschutzbeauftragter und Datenschutzvertreter

# Datenschutz-Folgeabschätzungen



- Vor Aufnahme der Datenbearbeitung ist eine Abschätzung der Folgen von Datenbearbeitungsvorgängen durchzuführen, wenn die Bearbeitung aufgrund
  - der Art, des Umfangs, der Umstände und der Zwecke oder
  - der Verwendung neuer Technologien

  voraussichtlich ein hohes Risiko für die Rechte der Betroffenen mit sich bringt.

  *Bsp.: Systematische und umfassende Bewertung persönlicher Aspekte von Personen, wie Profiling als Grundlage für Entscheidungen, die Rechtswirkungen gegenüber Betroffenen entfalten,* z.B. bei der *Frage, ob ein Kredit gewährt wird.*

  *Bsp.: Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche, z.B. mittels Videoüberwachung.*

# Datenschutz-Folgeabschätzungen



- Prüfungsschritte
  1. Voraussetzungen für Durchführung der Datenschutz-Folgenabschätzung erfüllt?
  2. Festlegung von Datenarten und Rechtsgrundlage
  3. Prüfung Einhaltung datenschutzrechtlicher Grundsätze
  4. Konsultation des Datenschutzbeauftragten (wenn vorhanden)
  5. Beschreibung der geplanten Verarbeitungsvorgänge
  6. Untersuchung der Risiken für Datensicherheit (Verfügbarkeit, Integrität und Vertraulichkeit), Zweckbindung, Rechte und Freiheiten der Betroffene
  7. Risikobewertung nach identifizierten Risiken (Eintrittswahrscheinlichkeit/Folgen)
  8. Festhalten der bisher getroffenen Abhilfemassnahmen
  9. Aufstellung eines Massnahmeplans

# Datenschutz-Folgeabschätzungen



- Inhalt
  - Geplante Verarbeitungsvorgänge, Verarbeitungszwecke, Berechtigte Interesse, Notwendigkeit und Verhältnismässigkeit
  - Risiken für Rechte und Freiheiten der Betroffenen
  - Die zur Bewältigung der Risiken geplanten Abhilfemassnahmen, einschliesslich Garantien, Sicherheitsvorkehrungen und Verfahren
  - Empfehlungen des Datenschutzbeauftragten und Entscheidungen dazu

- Konsultation der Aufsichtsbehörde, wenn Risiko nicht beschränkt werden kann

# Anforderungen, die man kennen muss

1. Bearbeitungsgrundsätze
2. Rechtfertigungsgrund, Einwilligung
3. Informationspflicht, Betroffenenrechte
4. Technische und organisatorische Massnahmen
5. Datenschutz-Folgeabschätzung
6. Accountability
7. Meldungen von Datenschutzverletzungen
8. Datenübermittlung ins Ausland
9. Datenschutzbeauftragter und Datenschutzvertreter

# Accountability



Verantwortlicher trägt Beweislast für Einhaltung der Bearbeitungsgrundsätze. Der Compliance-Nachweis schliesst *Dokumentationspflichten* ein:

1. Verzeichnis der Bearbeitungstätigkeiten
   - Inhalt: Kontaktdaten; Zwecken; Kategorien von Daten, Betroffenen, Empfängern; int. Datentransfer; Speicherfrist; Technischen u. organisatorischen Massnahmen
   - Pflicht für Unternehmen mit weniger als 250 Mitarbeitern nur dann nicht, wenn
     - Kein Risiko für Betroffene
     - Nur gelegentliche Verarbeitung
     - Keine sensible Datenkategorien
2. Datenschutz-Folgeabschätzung
3. Getroffene Schutzmassnahmen

# Anforderungen, die man kennen muss

1. Bearbeitungsgrundsätze
2. Rechtfertigungsgrund, Einwilligung
3. Informationspflicht, Betroffenenrechte
4. Technische und organisatorische Massnahmen
5. Datenschutz-Folgeabschätzung
6. Accountability
7. Meldungen von Datenschutzverletzungen
8. Datenübermittlung ins Ausland
9. Datenschutzbeauftragter und Datenschutzvertreter

# Privacy Breach



- Verstösse gegen Datenschutzmassnahmen bzw. Sicherheitslücken (in der Regel Vorfälle, durch die Unbefugten der Zugriff auf Daten möglich wird) sind innert 72 Stunden an die zuständige Aufsichtsbehörde zu melden, wenn Auswirkungen auf Betroffene möglich sind (voraussichtliches Risiko für ihre Rechte).

- Inhalt Meldung:
  - Art Verletzung
  - Wahrscheinliche Folgen Verletzung
  - Ergriffene und vorgeschlagene Massnahmen

- Dokumentationspflicht über alle Fakten (Auswirkungen, Massnahmen usw.)

- Betroffene unverzüglich und in einfacher und klarer Sprache zu informieren, wenn voraussichtlich ein hohes Risiko für deren Rechte besteht

# Anforderungen, die man kennen muss

1. Bearbeitungsgrundsätze
2. Rechtfertigungsgrund, Einwilligung
3. Informationspflicht, Betroffenenrechte
4. Technische und organisatorische Massnahmen
5. Datenschutz-Folgeabschätzung
6. Accountability
7. Meldungen von Datenschutzverletzungen
8. Datenübermittlung ins Ausland
9. Datenschutzbeauftragter und Datenschutzvertreter

# Auslanddatentransfer



1. Schutzniveau im Zielland
   - Angemessenheitsentscheid
   - Vertragliche Garantien (EU-Standardverträge)
   - Behördlich genehmigte Binding Corporate Rules
   - Behördlich genehmigte Verhaltensregeln/Zertifizierungsmechanismus
2. Einwilligung des Betroffenen
3. Zur Erfüllung eines Vertrags erforderlich
4. Zur Wahrung der zwingenden berechtigten Interessen des Verantwortlichen falls
   - Überwiegende Interessen
   - Geeignete Garantien für konkrete Umstände
   - Keine wiederholte Übermittlung und nur begrenzte Zahl von Betroffenen
   - Aufsichtsbehörde und Betroffene in Kenntnis gesetzt

# Anforderungen, die man kennen muss

1. Bearbeitungsgrundsätze
2. Rechtfertigungsgrund, Einwilligung
3. Informationspflicht, Betroffenenrechte
4. Technische und organisatorische Massnahmen
5. Datenschutz-Folgeabschätzung
6. Accountability
7. Meldungen von Datenschutzverletzungen
8. Datenübermittlung ins Ausland
9. Datenschutzbeauftragter und Datenschutzvertreter

# Datenschutzbeauftragter



- Ernennungspflicht:
  - Kerntätigkeit sind Vorgänge, die regelmässige, systematische und umfangreiche Verhaltenstracking von Betroffenen erfordern (aufgrund ihrer Art, ihres Umfanges und/oder ihrer Zwecke – *z.B. Banken, Versicherungen, Kreditauskunfteien und Berufsdetektive*) oder
  - Kerntätigkeit ist umfangreichen Verarbeitungen sensibler Personendaten, *z.B. Big-Data-Analysen oder bei Krankenanstalten*.
- Qualifiziert, unabhängig
- Unterrichtet, berät, überwacht, Anlaufstelle für Behörden und Betroffene

# Datenschutzvertreter



- Verantwortliche und Auftragsverarbeiter ohne Niederlassung in der EU (die sich aber im Geltungsbereich der DGSVO befinden) müssen einen Vertreter in EU ernennen.
- Vertreter in einem der EU-Mitgliedstaaten niedergelassen, in denen sich die Betroffenen befinden.
- Ansprechperson für Betroffenen und Aufsichtsbehörden
- Ausnahmen:
  - Verarbeitung nur gelegentlich
  - Nicht umfangreiche Verarbeitung von sensiblen Daten oder Gesundheitsdaten
  - Voraussichtlich kein Risiko für Rechte der Betroffenen

# Rechtsfolgen bei Verstössen

# Rechtsfolgen



- Bei Verstössen gegen den materiellen Datenschutz:

  Geldbussen bis zu EUR 20 Mio. oder 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres des Unternehmens

- Bei Verstössen gegen Datenschutz-Governance und den Kinderdatenschutz:

  Geldbussen bis zu EUR 10 Mio. oder 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres des Unternehmens

- Behördliche Unterbindung von Datenbearbeitungen

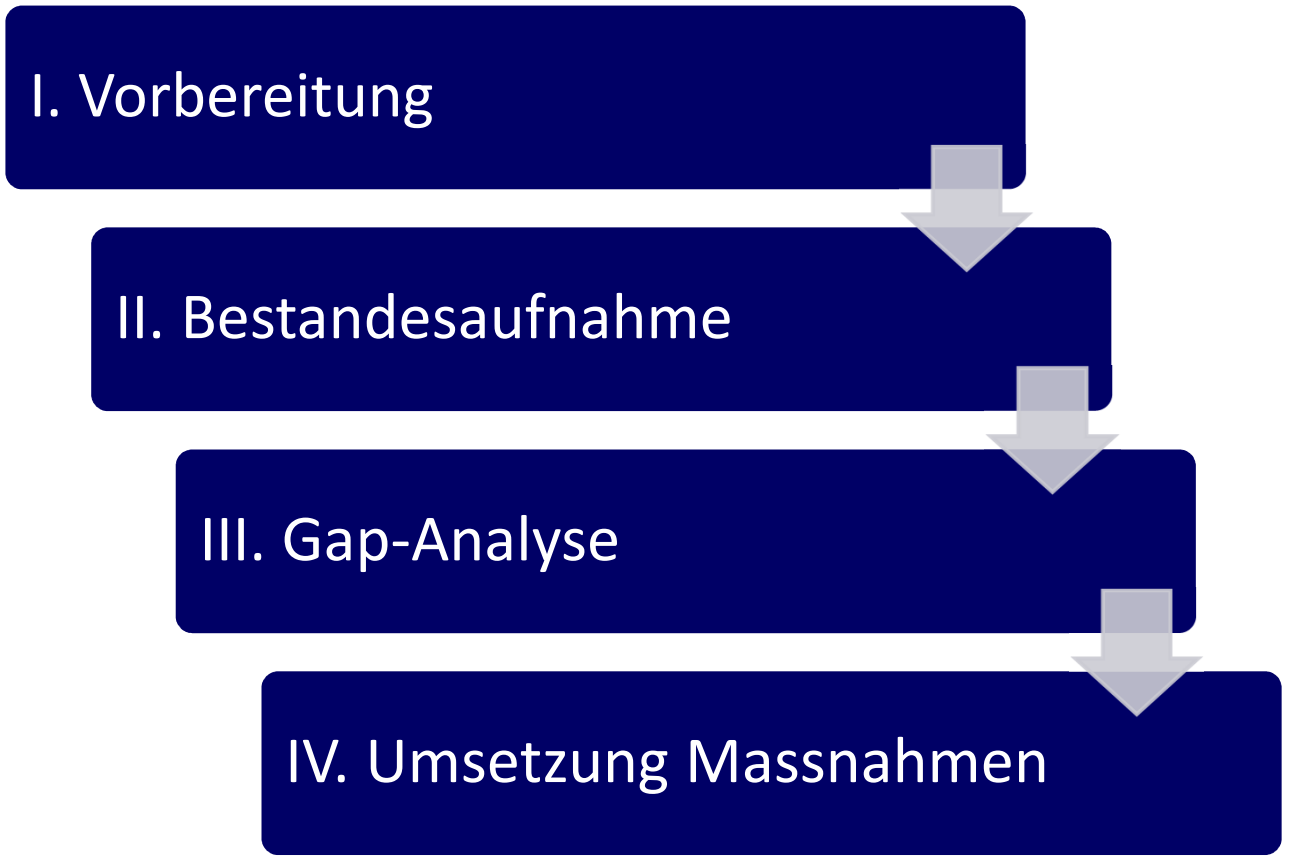
- Zivilrechtliche Ansprüche der Betroffenen (solidarische Haftung mit Regressrecht); Abmahnungen

- Verantwortlichkeitsklagen

# Handlungsbedarf

# Vorgehen




I. Vorbereitung
II. Bestandesaufnahme
III. Gap-Analyse
IV. Umsetzung Massnahmen

# I. Vorbereitung



- Schaffung eines Projekt-Teams (IT-, HR-, Legal-, Compliance- und Risk Management)
- Festlegung der Zuständigkeiten und der Projektorganisation
- Definition des Projektumfangs, der Ressourcen, des Budgets, des Zeitplans und der Mittel (Interviews, Questionnaires, Dokumentationssammlung, usw.).

# II. Bestandesaufnahme (Mapping)



1. Welche Personendaten bearbeitet werden (z.B. Mitarbeiter-, Kunden-, Lieferanten- oder sonstige Daten) und ob und welche sensiblen Daten
2. Wo sie behalten sind
3. Wer sie bearbeitet (z.B. Outsourcing der Bearbeitungsaktivitäten?)
4. Wie die Daten beschafft, verwendet, bearbeitet und behalten werden, z.B.
   - Bearbeitungsszenarien,
   - Profiling
   - Einhaltung der Bearbeitungsgrundsätze,
   - Rechtsgrundlage/Rechtfertigungsgründe und Einwilligungen,
   - Informationen an die Betroffenen,
   - Erfüllung der Betroffenenrechte,
   - Umsetzung von privacy by design/privacy by default,
   - Anonymisierung und Pseudonymisierung.

# II. Bestandesaufnahme (Mapping)



5. Ob Personendaten ins Ausland übermittelt werden sollen, wohin, Rechtsgrundlage
6. Welche technischen/organisatorischen Massnahmen zur Datensicherheit bestehen
7. Wie die interne Organisation und die Kontrollmechanismen aufgebaut sind
   - zuständige Abteilungen, Datenschutzbeauftragter?
   - Prozesse und Richtlinien
   - Datenschutzhinweise, Datenschutzerklärungen, Verträge mit Betroffenen
   - Verträge für die Auftragsverarbeitung
   - Anlaufstelle für Betroffene
   - Informationen und Schulungen
   - Dokumentation der Bearbeitungsart
   - Datenschutz-Folgenabschätzung durchzuführen? Risiken, Massnahmen?
   - Massnahmenüberprüfung, Datenschutzaudits

# II. Bestandesaufnahme (Mapping)



8. Nachweis der Einhaltung des Datenschutzrechts, z.B.
   - Dokumentation der Einwilligungserklärungen
   - Verarbeitungsverzeichnis
   - Dokumentation der ergriffenen Sicherheitsmassnahmen
   - Dokumentation der Risikoabschätzung
   - Protokollierung oder Dokumentation der Weisungen an dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Personen
   - Dokumentation der Verpflichtung der Mitarbeiter des Auftragsverarbeiters zur Vertraulichkeit, usw.

# III. Gap-Analyse



1. Definition der Anforderungen
2. Vergleich des Ist-Zustands mit den Anforderungen mittels einer datenbezogenen und organisationsbezogenen Analyse
3. Erstellung eines Massnahmenplans (Zeitplan, Budget) nach risikobasiertem Ansatz
4. Priorisierung der Massnahmen

# IV. Umsetzung



1. Schaffung von Strukturen und Umsetzung der Anforderungen
2. Erstellung der Prozesse, z.B.
   - Zweckfestlegung und Zweckänderung
   - Privacy by design
   - Verarbeitungsverzeichnis
   - Profiling, Big Data-Analyse
   - Datenschutz-Folgeabschätzung
   - Auftragsverarbeitung
   - Ausübung der Betroffenenrechte
   - Internat. Datentransfer
   - Datensicherheit
   - Datenübertragbarkeit
   - Verstösse
3. Ausarbeitung der erforderlichen Dokumentation
4. Trainings
5. Kontrollen

# Erforderliche Massnahmen im Einzelnen



1. Schaffung eines **Datenschutzkompetenzzentrums** innerhalb des Unternehmens und, wenn erforderlich, Ernennung eines Datenschutzbeauftragten und eines Datenschutzvertreters in der EU

2. Eventuelle Einstellung oder Anpassung der bestehenden **Datenbearbeitungen** sowie Einführung oder Anpassung der entsprechenden Prozesse und Richtlinien (z.B. betreffend Zweckfestlegung und -änderung, Profiling, Big Data-Analyse),

3. Festlegung von Prozessen zur **Prüfung von neuen Datenbearbeitungen**, inkl. Privacy by Design und Privacy by Default, d.h. Beizug von Datenschutzspezialisten bei der Entwicklung und Ausgestaltung aller neuen Produkte, Dienste und Anwendungen mit Datenbearbeitungsmerkmalen

# Erforderliche Massnahmen im Einzelnen



3. Festlegung des **Rahmens für die "Accountability"**, insbesondere durch
   - Nachweis der Compliance mit den Datenschutzgrundsätzen,
   - Erstellung einer Liste mit allen Datenbearbeitungen (Verarbeitungsverzeichnis),
   - betriebsinterne Informationen und Schulungen,
   - Entwicklung einer Kultur der Verhältnismässigkeit und Minimierung der Datenbearbeitungen und Datensammlungen,
   - Datenschutz-Folgeabschätzungen und
   - laufende Überprüfung, Überarbeitung und Auditierung der Risikoanalysen, inklusive der jeweiligen Prozesse und Richtlinien

4. Umfassende **Information** der Betroffenen; Prüfung und Anpassung von Datenschutzerklärungen und -hinweisen sowie von Verträgen mit Betroffenen und sonstigen Informationen

# Erforderliche Massnahmen im Einzelnen



5. Einholung der **Einwilligungen**; Prüfung, ob bisherige Einwilligungsdokumente geeignet und angemessen sind sowie ob Einwilligungen freiwillig erteilt wurden.
6. Festlegung oder Anpassung von Prozessen und Richtlinien für **Betroffenenrechte**; Technische Implementierung von Datenlöschungen, -minimierung und -portabilität.
7. Abschluss bzw. Überprüfung und Anpassung von **Verträgen mit sorgfältig ausgewählten Auftragsdatenbearbeitern** sowie von entsprechenden Prozessen und Richtlinien.
8. Erstellung oder Anpassung von Verträgen über den **Auslandsdatentransfer** und Binding Corporate Rules sowie von entsprechenden Prozessen und Richtlinien.

# Erforderliche Massnahmen im Einzelnen



9. Anpassung der technischen und organisatorischen **Sicherheitsmassnahmen** und der entsprechenden Richtlinien und Prozesse (Pseudonymisierung personenbezogener Daten, Sicherung von Integrität, Vertraulichkeit der Daten, unverzügliche Verfügbarkeit von und Zugriff auf Personendaten, Prozess zur regelmässigen Prüfung der Effektivität der technischen und organisatorischen Sicherheitsmassnahmen).

10. Erstellung von Prozessen und Richtlinien zur Sicherstellung schneller **Reaktionsmassnahmen** im Fall von Datenschutzverstössen.

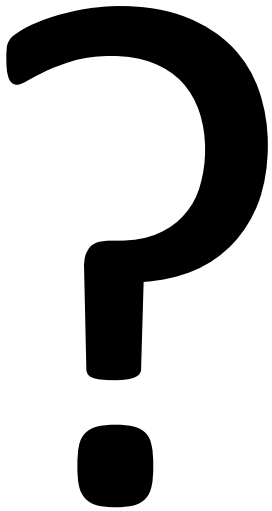
# Beispiel für Teil-Projekt Webseite



- ☐ Evaluieren, welche Daten, woher, zu welchen Zwecken, wie lange erhoben/verarbeitet werden.
- ☐ Abschluss Vertrags zur Auftragsverarbeitung mit Dienstleistern (Hoster, E-Mail-Marketing Software, Tracking Software usw.).
- ☐ Prüfen, ob der Dienstleister den gesetzlichen Anforderungen entspricht (Nachweis vom Verarbeiter).
- ☐ Hinweis auf Datenschutzerklärung bei Registrierung für Newsletter und Einwilligung (evtl. Checkbox).
- ☐ Datenschutzerklärung anpassen oder erstellen.
- ☐ Erforderlichenfalls mit Einwilligungen arbeiten.
  - Evaluieren, ob Einwilligung alle erhobenen Daten, Anwendungen, Zwecke genau umfasst.
  - Keine vorangekreuzten Check-Boxen verwenden.
  - Nachweis der Einwilligung zum Newsletter (Adresse, Datum, Uhrzeit) von allen Empfängern.
- ☐ Altersgrenzen setzen.
- ☐ Website nach Stand der Technik möglichst sicher und datenschutzfreundlich konfigurieren.
- ☐ Website so erstellen, dass eine Datenübertragbarkeit möglich ist.
- ☐ Betriebsinternes Daten-Dokumentationssystem aufbauen.

# Also, alles sehr einfach!





Dr. Stefano Caldoro, LL.M., MLP-HSG
Rechtsanwalt, Partner

LANTER Anwälte & Steuerberater
Seefeldstrasse 19
8032 Zürich

T: +41 44 250 29 29
E-Mail: caldoro@lanter.biz