Kellerhals Carrard

Neuerungen des Datenschutzgesetzes

EXPERTsuisse Sektion Zürich,
Jahresversammlung vom 4. Juli 2023

Luca Stäuble

Einleitung

Warum wurde das DSG revidiert?

- Altes Gesetz von 1992, nicht mehr „zeitgemäss“
- Technologischer Fortschritt (Digitalisierung, Big Data)
- Anpassung an EU-Umfeld (Gewährleistung Datenfluss, Wettbewerbsfähigkeit)

Entwicklung Gesetzgebung

Entwurf E-DSG und Botschaft

Inkrafttreten EU-DSGVO

Verabschiedung Totalrevision DSG

Inkrafttreten nDSG (ohne Übergangsfristen)

Datenschutz

Was sind Personendaten?

*«Angaben, die sich auf eine **bestimmte oder bestimmbare** **natürliche** **Person** beziehen.»*

Anonymisierte Personendaten

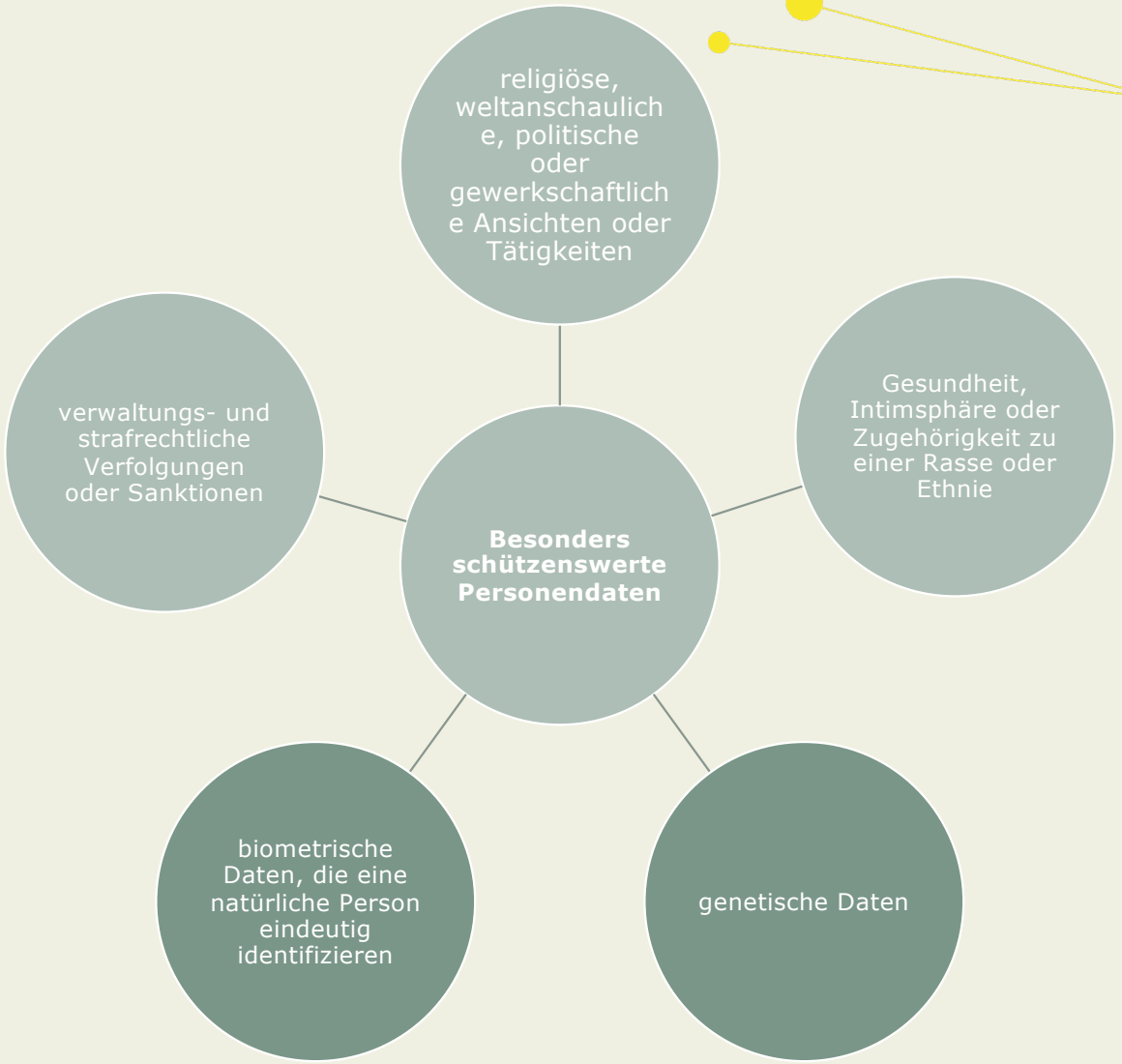
- Unwiderrufliche Aufhebung des Personenbezugs
- In der Praxis: Schwärzung von Dokumenten
- Keine Rückschlüsse auf eine natürliche Person mehr möglich

➢ ***Keine*** Personendaten

Pseudonymisierte Personendaten

- Ersetzung von identifizierenden Merkmalen z.B. durch Nummern
- Schlüssel zur Re-Identifizierung ist separat aufbewahrt und gesichert
- Relativer Ansatz (CH): Perspektive des Datenempfängers entscheidend

➢ Personendaten


religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten
verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen
Gesundheit, Intimsphäre oder Zugehörigkeit zu einer Rasse oder Ethnie
Besonders schützenswerte Personendaten
biometrische Daten, die eine natürliche Person eindeutig identifizieren
genetische Daten

Rechtsfolgen

Weitergabe an Dritte (nicht: Auftragsbearbeiter)

- Stellt grundsätzlich eine Persönlichkeitsverletzung dar
- Setzt eine Rechtfertigung (z.B. Einwilligung, überwiegendes Interesse, Gesetz) voraus

Risikoaspekte (Pflichten bei umfangreicher Bearbeitung)

- Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung
- Keine Ausnahme zur Führung eines Bearbeitungsverzeichnis
- Datensicherheit: Pflicht zur Protokollierung und Führung eines Bearbeitungsreglements

Was ist eine Datenbearbeitung?

- Beschaffung (bei betroffener Person oder bei Dritten)
- Speicherung
- Aufbewahrung
- Verwendung
- Veränderung und -auswertung
- Weitergabe
- Vernichtung, Anonymisierung
- …

Profiling

- eine **Bearbeitung** von Personendaten,
- die **automatisiert** erfolgt, und zwar,
- mit dem Ziel einer **Bewertung persönlicher Aspekte**.

z.B. Personalisierung von Angeboten für Kunden

Rechtsfolgen

- Grundsatz: Information gegenüber betroffenen Personen (z.B. in Datenschutzerklärung)
- Keine Ausnahme zur Führung eines Bearbeitungsverzeichnis
- Datensicherheit: Pflicht zur Protokollierung und Führung eines Bearbeitungsreglements

Verantwortlicher

- Entscheidet über den Zweck und die Mittel der Bearbeitung von Personendaten
- Auch gemeinsame Verantwortlichkeit durch zwei oder mehr Bearbeiter möglich

z.B. Wirtschaftsprüfer, Anwälte

Auftragsbearbeiter

- Bearbeitet Personendaten im Auftrag und demnach auf Weisung des Verantwortlichen
- Auslagerung einer «eigenen» Datenbearbeitung des Verantwortlichen

z.B. Cloud-Provider

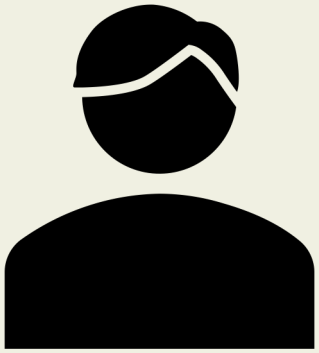
Datenschutz

Grundsätze der Datenbearbeitung

- Bearbeitung zulässig, sofern Grundsätze eingehalten sind
- Verletzung kann gerechtfertigt werden (z.B. Einwilligung, überwiegende Interessen, Gesetz)
- Bindet Verantwortliche und Auftragsbearbeiter
- Nicht sanktionsbedroht

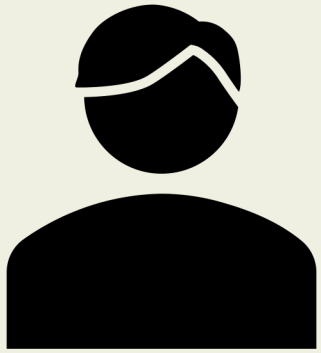
Treu und Glauben

„Tue nichts, was du als betroffene Person nicht akzeptieren würdest“



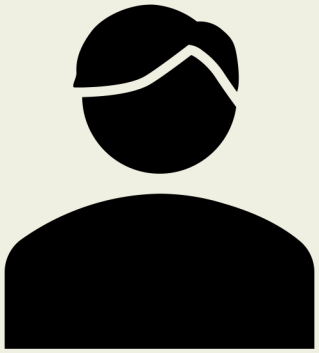
Verhältnismässigkeit

„Beschaffe und verwende nur so viele Daten, wie notwendig“



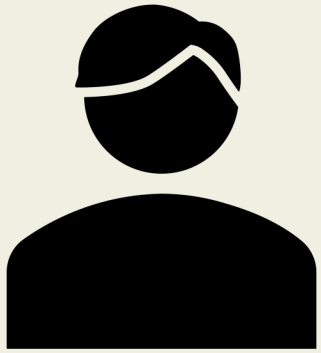
Zweckbindung

„Halte dich an die Zwecke, die du mit der Bearbeitung verfolgst“



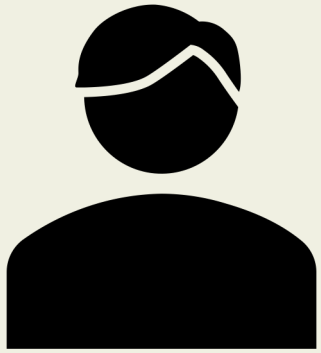
Transparenz

„Bearbeite Daten nicht heimlich. Teile den Betroffenen mit, woher du die Daten hast, wozu du sie verwendest und wem du sie weitergibst“



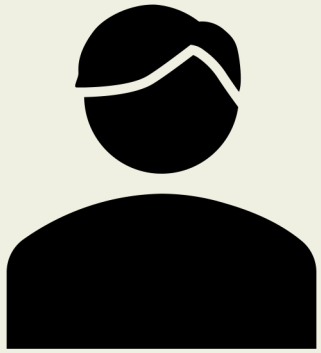
Datenrichtigkeit

„Korrigiere falsche Daten“



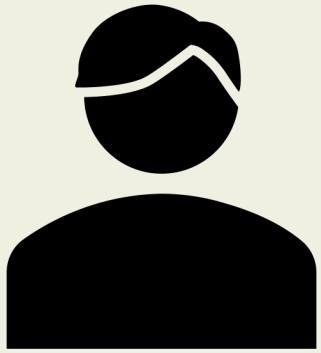
Datenlöschung

„Lösche oder anonymisiere Daten, die du nicht mehr brauchst“



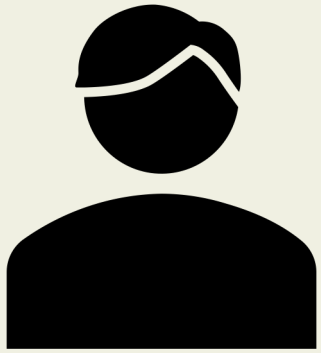
Privacy by Default

„Konfiguriere die Voreinstellungen so, dass möglichst wenig Daten bearbeitet werden“



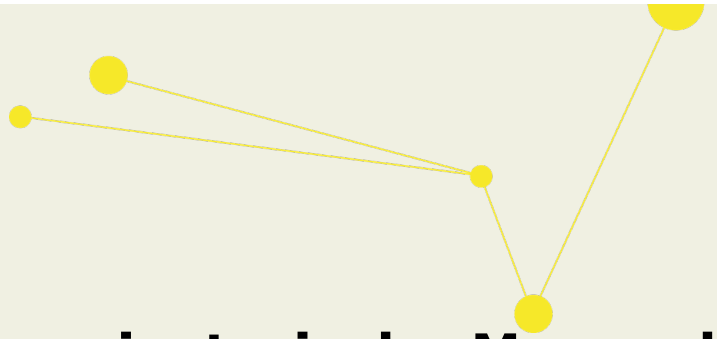
Privacy by Design

„Gestalte die Datenbearbeitung so, dass der Datenschutz eingehalten werden kann “



Gewährleistung der Datensicherheit

- Geeignete technische und organisatorische Massnahmen («TOMs»)
- Risikobasierter Ansatz (Art und Bearbeitung von Personendaten, deren Weitergabe etc.)
- Sanktionsbedroht



Technische Massnahmen

- Pseudonymisierung
- Automatische Datenlöschung
- Rollenbasierte Zugriffsrechte
- Datenprotokollierungen (Logs)
- Backups
- Firewall
- …

Organisatorische Massnahmen

- Weisungen
- Geheimhaltungsverpflichtungen
- Schulung von Mitarbeitenden
- Zugriffs- und Löschkonzepte
- Umsetzungskontrollen
- Prozesse (z.B. Auskunftsbegehren)
- …

Schutzziele: Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit

Meldepflicht bei Verletzungen der Datensicherheit

- Meldung an **EDÖB**, falls die Verletzung der Schutzziele voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt.
- Meldung „so rasch als möglich" mit Mindestinhalt gemäss Gesetz.
- Information der **betroffenen Person**, wenn zu ihrem Schutz erforderlich oder EDÖB es verlangt.
- Aufbewahrungspflicht: zwei Jahre.
- Nicht sanktionsbedroht.

Bearbeitungsverzeichnis

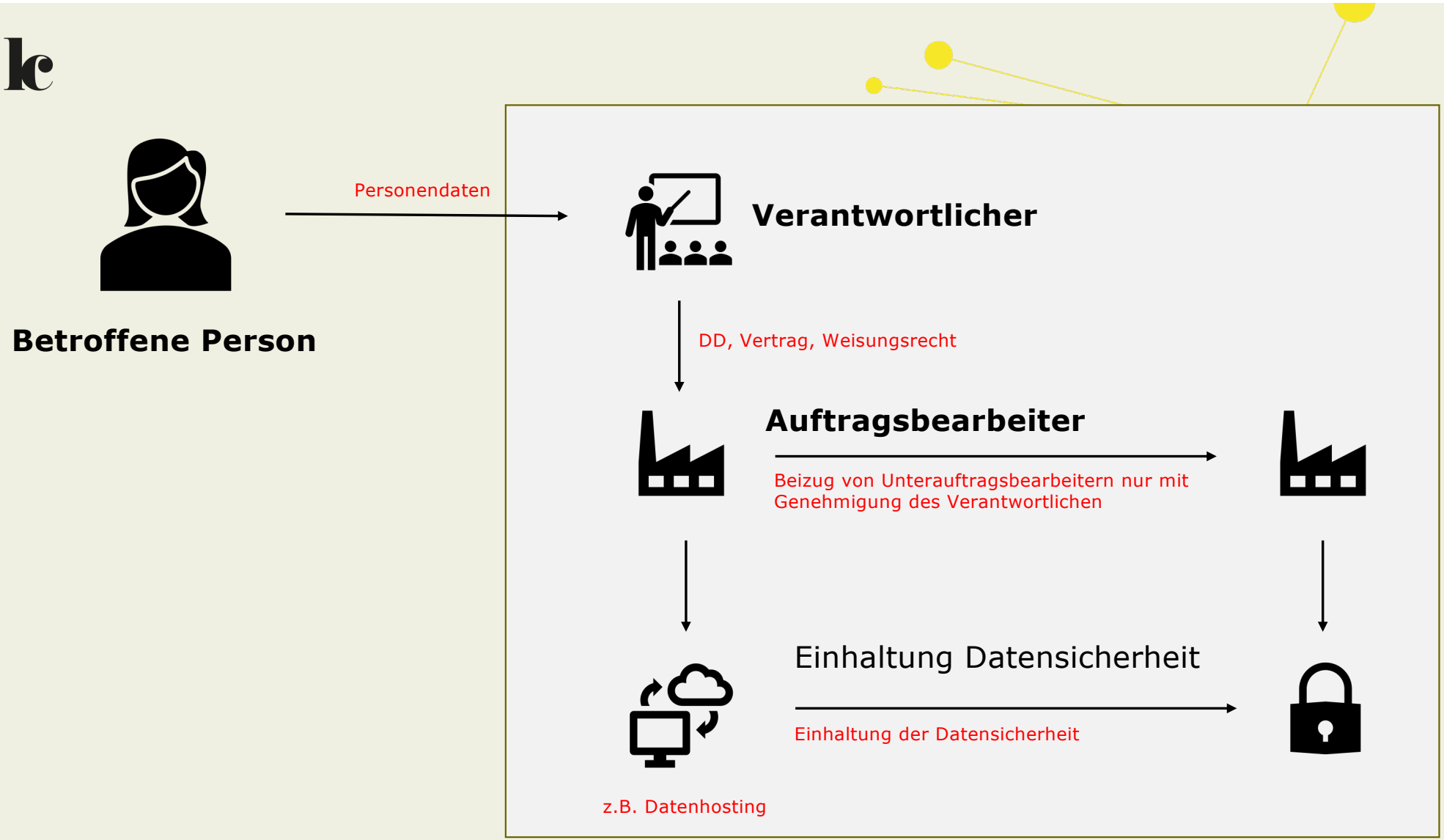
- Mindestinhalt Verantwortlicher:
  - Identität
  - Zweck der Bearbeitung
  - Kategorie betroffene Personen
  - Kategorie betroffene Daten
  - Kategorie Empfänger
  - Aufbewahrungsdauer
  - TOMs
  - Auslandtransfers / ggf. Garantien
- Mindestinhalt Auftragsbearbeiter:
  - Identität (inkl. Verantwortlicher)
  - Kategorie Bearbeitungen
  - TOMs
  - Auslandtransfers / ggf. Kategorien
- KMU-Ausnahme (< 250 MA)
- Nicht sanktionsbedroht

Informationspflichten

- Pflicht des Verantwortlichen
- i.d.R. im Zeitpunkt der Beschaffung
- Mindestinhalt:
  - Identität des Verantwortlichen
  - Bearbeitungszweck
  - ggf. Kategorie von Empfängern
  - ggf. Kategorie von Personendaten
  - ggf. Länder und Garantien
  - ggf. Sonderfall «AEE»
- Datenschutzerklärung, z.B.
  - auf Webseite
  - Anhang zu Vertrag
  - Personalreglement (für MA)
- Ausnahmen/Einschränkungen
- Sanktionsbedroht

Auftragsbearbeitung

- Auftragsbearbeiter muss Personendaten nach Weisung des Verantwortlichen bearbeiten
- Auftragsbearbeitung darf nicht gesetzlich oder vertraglich verboten sein
- der Verantwortliche muss sich vergewissern, dass der Auftragsbearbeiter die Datensicherheit zu gewährleisten vermag (Due Diligence)
- der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Zustimmung des Verantwortlichen einem Dritten übertragen → generell oder explizit
- Schriftlicher Vertrag («ADV») mit Regelungsinhalt analog Mindestinhalt DSGVO (Auditrechte etc.)
- Sanktionsbedroht


Personendaten
Verantwortlicher
Betroffene Person
DD, Vertrag, Weisungsrecht
Auftragsbearbeiter
Beizug von Unterauftragsbearbeitern nur mit Genehmigung des Verantwortlichen
Einhaltung Datensicherheit
Einhaltung der Datensicherheit
z.B. Datenhosting

Prüfschritte

1 **Rollen**

Prüfe, ob dein Dienstleister ein Auftragsbearbeiter ist: erfolgt die Bearbeitung in deinem Auftrag und nach deinen Anweisungen, handelt es sich in Bezug auf die Datenbearbeitungen um deinen «verlängerten Arm»?

2 **Zulässigkeit**

Stelle sicher, dass die Auftragsbearbeitung nicht gesetzlich oder vertraglich verboten ist.

3 **Due Diligence**

4 **Vertrag**

Vergewissere dich, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten. Fordere den Auftragsbearbeiter auf, dir seine TOMs darzulegen sowie allfällige Auslandtransfers offenzulegen.

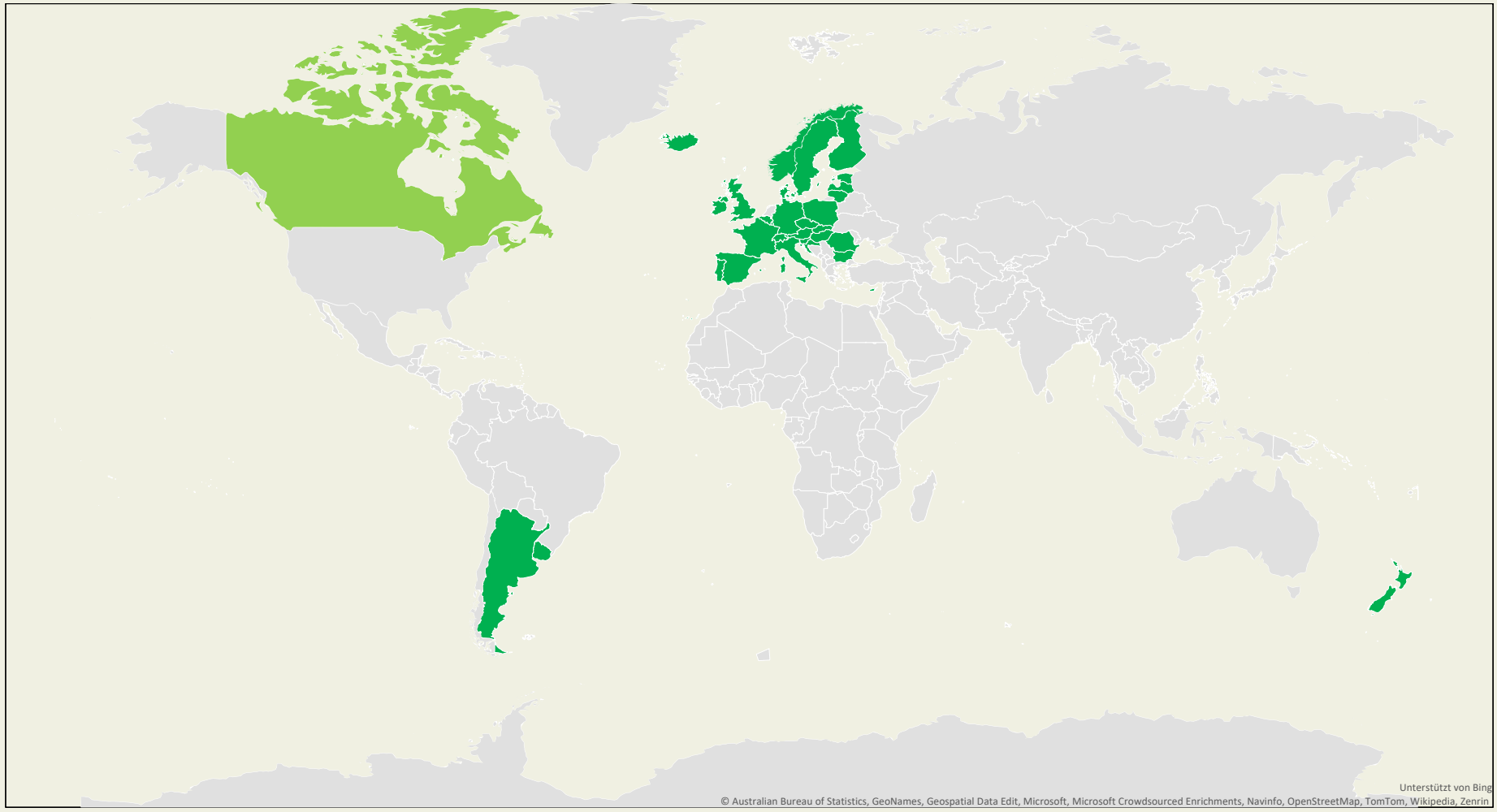
Befindet sich der Dienstleister in einem «unsicheren» Drittland: Führe ein Transfer Impact Assessment («**TIA**») durch und triff zusätzliche Massnahmen.

Schliesse einen schriftlichen Vertrag (**ADV**) ab, der die wichtigsten Aspekte der Auftragsbearbeitung regelt (insb. Weisungsrecht, TOMs, Genehmigungspflicht Unterbeauftragung, Auditrechte, Haftung).

Auslandtransfers

- Bekanntgabe von Personendaten ins Ausland ist zulässig, wenn dort ein angemessener Datenschutz besteht
- Bundesrat legt die “sicheren“ Länder fest (siehe Anhang 1 zur DSV)
- Bekanntgabe in „unsichere“ Länder ist unter anderem möglich mit sog. Standardvertragsklauseln („SCC“)
- ABER: Durchführung einer Risiko-beurteilung im Einzelfall und ggf. weitere Massnahmen erforderlich
- Ausnahmen möglich: Einwilligung oder Vertragsabwicklung, weitere

Länderliste



Auslandtransfers

«Sicheres» Drittland

- Empfängerland verfügt über angemessenes Datenschutzniveau
- Siehe Länderliste des Bundesrats in Anhang 1 der DSV

TIA und Garantien

- Durchführung Transfer Impact Assessment (TIA), um die Risiken, insb. von Behördenzugriffen, zu identifizieren (gemeinsam mit Datenempfänger)
- Standardvertragsklauseln abschliessen und ggf. weitere Massnahmen treffen ODER absehen von Datentransfer («Null-Risiko-Ansatz»)

Ausnahmen

- Einwilligung der betroffenen Person
- Abwicklung eines Vertrags mit oder im Interesse der betroffenen Person
- Notwendigkeit für die Wahrung öffentlicher Interessen
- Wahrung von Rechten
- ….

Datenschutz-Folgenabschätzung (DSFA)

- Pflicht des Verantwortlichen zur Identifizierung, Bewertung und Mitigierung von Datenschutzrisiken
- Falls eine Bearbeitung ein hohes Risiko für die betroffenen Personen mit sich bringen kann
- Bei ähnlichen Bearbeitungsvorgänge kann eine gemeinsame Abschätzung erstellt werden
- Indizien für hohes Risiko: Neue Technologien, Art, Umfang, Umstände und Zweck der Bearbeitung (z.B. umfangreiche Bearbeitung besonders schützenswerter Personendaten)
- Inhalt: Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die betroffenen Person sowie die Schutzmassnahmen (TOMs)
- Nicht sanktionsbedroht

Betroffenenrechte

- Rechte zur „Kontrolle“ von Datenbearbeitungen:
  - Auskunft
  - Datenportabilität
  - Berichtigung
  - Löschung
- Ausnahmen/Einschränkungen
- Modalitäten, z.B.
  - Identifizierung
  - 30-Tagesfrist
  - Kostenlosigkeit
- Falls Auskunft vorsätzlich falsch oder unvollständig: sanktionsbedroht

Sanktionen

- Katalog strafbewehrter Pflichten
- Strafbarkeit der verantwortlichen natürlichen Person (nicht: Unternehmen)
- (Eventual-)Vorsatz erforderlich
- Strafantrag der betroffenen Person
- Busse bis max. CHF 250‘000

Katalog strafbewehrter Pflichten

Allgemein

- Informationspflichten
- Auskunftspflichten
- Mitwirkungspflichten (z.B. bei Verfügungen des EDÖB)

Sorgfaltspflichten

- Verletzung der Mindestanforderungen an die Datensicherheit
- Mangelhafte Überprüfung von Auftragsbearbeitern
- Übermittlung von Daten in Drittstaaten

Berufliche Schweigepflicht

- Offenbarung von geheimen Personendaten, welche man in Ausübung seines Berufes zur Kenntnis genommen hat, an Unberechtigte
- Nur wenn in Erwartung anvertraut, dass diese «geheim bleiben»

- Bearbeitungsverzeichnis erstellen und pflegen
- Besonders schützenswerte Daten identifizieren und ggf. Massnahmen treffen
- Prozess für Erkennung und Meldung von Verletzungen der Datensicherheit
- Datenschutzerklärungen auf neue Vorgaben prüfen und ggf. anpassen
- Prozess für Beantwortung von Auskunftsgesuchen implementieren
- Angemessene TOMs implementieren und dokumentieren
- Auftragsbearbeitungen identifizieren und ggf. ADVs anpassen bzw. abschliessen
- Aufbewahrungsrichtlinie erarbeiten und überwachen
- Datentransfers ins Ausland prüfen und Massnahmen (insb. TIA, SCCs) treffen

Kellerhals Carrard

Luca Stäuble, LL.M.

Rechtsanwalt, Senior Associate

Rämistrasse 5
Postfach
8024 Zürich

Tel. 058 200 39 41
luca.staeuble@kellerhals-carrard.ch