Summary zum CH DSG 2020

Summary zum CH Datenschutz-Gesetz 2020

DSG Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)
vom 25. September 2020

DSV Verordnung über den Datenschutz (Datenschutzverordnung, DSV)
vom 31. August 2022

DSV-E Verordnung über den Datenschutz (Datenschutzverordnung, DSV)
vom 31. August 2022 (Erläuternder Bericht)

Art. 2 EU DSGVO «Sachlicher Anwendungsbereich»
– keine konkrete Beschreibung in CH-Gesetz und CH-Verordnung
Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die **in einem Dateisystem gespeichert sind oder gespeichert werden sollen**.
(Gilt sinngemäss auch für die Schweiz – wie soll man Papier mit TOM's sinnvoll schützen? Bei der Review des Gesetzes sowie der Verordnung war kein Hinweis auf «Papier-Personendaten» ersichtlich)

Art. 5 DSG Definitionen
Begriffe In diesem Gesetz bedeuten:
a. Personendaten: alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen;
b. betroffene Person: natürliche Person (in der Schweiz), über die Personendaten bearbeitet werden;
c. besonders schützenswerte Personendaten (Spezialfall Profiling und Protokollierung s. am Ende):

1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,
3. genetische Daten,
4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,
5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
6. Daten über Massnahmen der sozialen Hilfe;

d. **Bearbeiten**: jeder Umgang mit Personendaten, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten;
e. Bekanntgeben: das Übermitteln oder Zugänglichmachen von Personendaten; **(auch Auftragsbearbeiter/Auftragsverarbeiter)**
f. Profiling: jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden zur Bewertung bestimmter persönlicher Aspekte……
g. Profiling mit hohem Risiko: Profiling, …. welches zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt;

j. **Verantwortlicher:** Private Person welche über den Zweck und die Mittel der Bearbeitung entscheidet
k. Auftrags**be**arbeiter: Private Person welche im Auftrag des Verantwortlichen Personendaten bearbeitet

h. **Verletzung der Datensicherheit**: …… Personendaten werden unbeabsichtigt oder widerrechtlich, gelöscht, vernichtet oder verändert oder Unbefugten offengelegt/zugänglich gemacht;

Art. 6 DSG Grundsätze Ausschnitt
(s. auch Erläuterungen zur Verordnung 31. Aug. 2022)

- Personendaten müssen rechtmässig bearbeitet werden (Art. 6 Abs. 1).
- Die Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein (Art. 6 Abs. 2).
- Personendaten dürfen nur zu einem **bestimmten und für die betroffene Person erkennbaren Zweck** beschafft werden (Art. 6 Abs. 3).
- Die Daten müssen vernichtet oder anonymisiert werden, **sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind** (Art. 6 Abs. 4).
- Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern (Art. 6 Abs. 5).
- Der Verantwortliche und der Auftragsbearbeiter sind verpflichtet, Personendaten durch Technik und datenschutzfreundliche Voreinstellungen zu schützen («privacy by design and by default»; Art. 7)
- und die Datensicherheit zu gewährleisten (Art. 8).

Art. 1 DSV Schutzbedarf der Personendaten
(Neu 2022 – war im DSG 2020 nicht enthalten)
Nachstehend die konkrete Massnahmenbeschreibung (1 von 42 Controls) aus dem **OBSERVAR Modul Massnahmen**:
Wir bestimmen den Schutzbedarf (Risiko) der Personendaten.
Wir gewährleisten eine angemessene Datensicherheit dieser Personendaten.
Wir als Verantwortliche sowie unsere Auftragsbearbeiter legen die geeigneten technischen und organisatorischen Massnahmen fest.
Der Schutzbedarf der Personendaten wird nach den folgenden Kriterien beurteilt:

a. Art der bearbeiteten Daten;
b. Zweck, Art, Umfang und Umstände der Bearbeitung.

Das Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person wird nach den folgenden Kriterien beurteilt:

a. Ursachen des Risikos;
b. hauptsächliche Gefahren;
c. ergriffene oder vorgesehene Massnahmen, um das Risiko zu verringern;
d. Wahrscheinlichkeit und Schwere einer Verletzung der Datensicherheit trotz der ergriffenen oder vorgesehenen Massnahmen.

Der Schutzbedarf der Personendaten, das Risiko und die technischen und organisatorischen Massnahmen sind über die gesamte Bearbeitungsdauer hinweg zu überprüfen. Die Massnahmen sind nötigenfalls anzupassen.

Informationspflichten
Personen müssen darüber informiert werden, dass deren Daten bearbeitet werden.
Datenschutzerklärung z.B. auf Website oder bei jeder Transaktion.

Inhalt der Datenschutz-Erklärung:
• Identität des Unternehmens (z. B. CHE-Nummer)
• Kontaktdaten des Unternehmens (E-Mail-Adresse)
• Rechte der betroffenen Person (Auskunftsrechte und Beschwerderechte)

Verzeichnis der Bearbeitungstätigkeiten (Pflicht gem. nDSG Art. 12)
(OBSERVAR Modul Bearbeitungstätigkeiten)
DSV 2.5 (Aug. 2022)
Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten
S. 12 KMU ohne risikobehaftete Datenbearbeitungen (DSV Art. 24) falls weniger als 250 MA

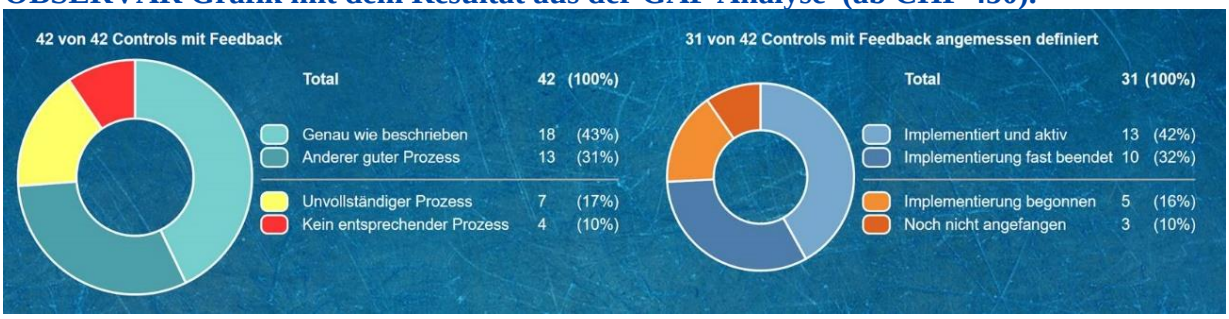
Ausnahme gilt nur, falls
a) nicht in grossem Umfang besonders schützenswerte Personendaten bearbeitet werden (Art. 5 DSG)
Definition «umfangreich» = grosse Mengen von Daten oder eine grosse Zahl von Personen betreffen
(aber nicht genau beziffert…)
b) kein Profiling mit hohem Risiko durchgeführt wird

Falls KMU < 250 MA (a) und b): Es müssen nicht alle Datenbearbeitungen im Verzeichnis geführt werden, nur die a) und b).

Verzeichnis pro Verfahren/Prozess
Strukturvorschlag OBSERVAR: Gliederung nach Applikationen
(nicht nach Prozessen) **(s. oben EU DSGVO Art. 2)**

DSV Art. 24 ab S. 50
Datensicherheit durch risikobasierten Ansatz (s. auch grosses OBSERVAR Summary)
(OBSERVAR Module Bearbeitungstätigkeiten und Modul Massnahmen Dokumentation und Aktualisierung/Einhaltung)
Artikel 8, Abs. 1: «Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische
Massnahmen eine dem Risiko angemessene Datensicherheit.»
Zentraler Artikel – Nichtbefolgung ist neu strafbedroht.
(OBSERVAR bietet Kunden eine GAP Analyse an mit 42 wichtigen/zentralen Themen welche eingehalten werden müssen)
Die gleichen 42 konkreten Massnahmen-Beschreibungen sind im Modul Massnahmen integriert)
Durchschnittlich 500 – 1'000 Zeichen konkrete griffige Massnahmen-Beschreibung für jedes der 42 Themen.
(Haben wir das? Halten wir das ein?)

OBSERVAR Grafik mit dem Resultat aus der GAP Analyse (ab CHF 450).



« privacy by design «
Je nach Risiko: angemessene technische und organisatorischen Massnahmen **(TOM nach Applikationen)** festzulegen
4 diese Massnahmen implementieren.
5 Risikoeinschätzung regelmässig auf ihre Aktualität prüfen.
Bei Bedarf – an neue Umstände anpassen.

Die korrekte Implementierung und Effektivität der TOM ist ebenfalls regelmässig zu überprüfen.
Dokumentation der erforderlichen Tätigkeiten damit in einem allfälligen Strafverfahren die gehörige Sorgfalt des Unternehmens (und somit auch der verantwortlichen Organe) belegt werden kann.
Es ist wichtig für die verantwortlichen Organe, dass **deren sorgfältiges Handeln dokumentiert wird**.
Entscheidend ist der sorgfältige, angemessene und bewusste Umgang mit Personendaten. Das Unternehmen darf angemessene Risiken eingehen.

Betroffenenrechte ***(OBSERVAR Modul Betroffenenrechte)***
Rechte der betroffenen Person gegenüber dem datenbearbeitenden Unternehmen.
Bedeutendstes Recht: **Auskunftsrecht.**
Zusätzlich: Recht auf Datenherausgabe oder Datenübertragung in einem gängigen elektronischen Format.
Entsprechende Auskünfte sind in der Regel **innert 30 Tagen** zu erteilen.
Eine ungenügende oder verspätete Auskunftserteilung ist in Zukunft strafbedroht.

Auskunfts- und Löschbegehren ***(OBSERVAR Modul Betroffenenrechte)***
Die korrekte Bearbeitung von Betroffenenrechten, insbesondere von Auskunfts- und Löschbegehren, ist sicherzustellen.
Eine Auskunft muss in der Regel innert 30 Tagen erfolgen.

Datenschutzvorfälle ***(OBSERVAR Modul Datenschutzvorfälle)***
Tritt eine Datenschutzverletzung ein (Datenschutzvorfall) müssen Meldepflichten eingehalten werden:

- Interne Alarmierung bei Datenschutzvorfällen.
- Innerhalb von 72 Stunden allfällige Meldung an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).
- Prüfung ob die betroffenen Personen zu informieren sind.
- Dokumentation der Vorgehensweise und Erfüllung der Informationspflichten

DSV Art. 4 + 5
Spezialfall «Protokollierung» sowie Spezialfall «Bearbeitungsreglement»
gilt für besonders schützenswerte Personendaten mit automatisierter Bearbeitung oder Profiling mit hohem Risiko
(s. grosses OBSERVAR Summary)

DSG 21
Spezialfall Informationspflicht bei einer automatisierten Einzelentscheidung
Ist für die meisten Industrieunternehmungen nicht relevant:
Nur falls: Entscheidungen mit einer Rechtsfolge werden automatisiert getroffen…

DSG 22
Spezialfall Datenschutz-Folgenabschätzung
Ist für die meisten Industrieunternehmungen selten relevant:
Falls eine geplante Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte betroffener Personen mit sich bringen kann – muss vorgängig eine Datenschutz-Folgenabschätzung erstellt werden. (z.B. umfangreiche Bearbeitung besonders schützenswerter Personendaten; oder systematische Überwachung öffentlicher Bereiche).

Strafbestimmungen gem. Datenschutz Art. 60ff (Ausschnitt)
- **Auf Antrag bis CHF 250'000**
- bei nicht wahrgenommenen Informations- und Auskunftspflichten / Mitwirkungspflichten (Vorsätzliche Unterlassung oder falsche oder unvollständige Auskunft)

Peter Nauer
Chief Executive Officer
Observar AG
Lindenstrasse 10
CH-6340 Baar / Zug, Switzerland

Mobile +41 79 344 75 19
peter.nauer@observar.ch
http://www.observar.ch