PROBSTPARTNER

Das neue DSG

Online-Seminar für den SVEB

Winterthur, 28. Juni 2023

Dr. Michael Widmer, LL.M.
Rechtsanwalt

Worum geht es?

Worum geht es? - Personendaten

Personendaten

Art. 5 lit. a DSG: «alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen»

Fakten und häufige Irrtümer zum neuen DSG

PROBSTPARTNER

Genau …

Das neue DSG tritt am 1. September 2023 ohne weitere Übergangsfrist in Kraft.

Ja: Es besteht eine Informationspflicht!

PROBSTPARTNER

Jedes Unternehmen benötigt eine Datenschutzerklärung.

PROBSTPARTNER

Irrtum

Die Bearbeitung von Personendaten ist nach DSG immer nur mit Einwilligung der betroffenen Personen zulässig.

PROBSTPARTNER

Es kommt darauf an...

Für den Versand von Newslettern ist eine Einwilligung erforderlich.

PROBSTPARTNER

Irrtum

Nach neuem DSG muss jedes Unternehmen eine Datenschutzberaterin benennen.

PROBSTPARTNER

Richtig,
mit Ausnahmen

Wenn eine betroffene Person es verlangt, muss ihr Auskunft über die bearbeiteten Personendaten erteilt werden.

PROBSTPARTNER

Es kommt darauf an …

Software von Anbietern aus den USA darf nach dem neuen DSG nicht benützt werden.

Die Umsetzung des DSG erfordert einen immensen Aufwand, bringt aber keinen Mehrwert.

PROBSTPARTNER

Folgen der Irrtümer?

Was sollten Sie wissen?

Was sollten Sie wissen?

Einige Neuerungen bei Folgen von DSG-Verletzungen

Ausbau der Ressourcen, Kompetenzen und Befugnisse des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)

Neu: Kostenlosigkeit von zivilrechtlichen Verfahren wegen Verletzung Persönlichkeit

Neu: strafrechtliche Bussen bis CHF 250’000 für gewisse Verletzungen von DSG-Vorschriften

- Täter ist grundsätzlich eine natürliche Person (Leitungsperson / Geschäftsführung)
- Nur vorsätzliche Pflichtverletzungen, aber so genannter Eventualvorsatz genügt
- Nicht gedeckt durch Versicherungen

Was sollten Sie wissen?

Nachfolgend konzentrieren wir uns auf: Was müssen Sie tun?

Insbesondere

- Kenntnis der Bearbeitungen erlangen und allenfalls *Bearbeitungsverzeichnis* erstellen
- Informationspflicht erfüllen, bspw. *Datenschutzerklärung*
- *Verträge* prüfen und allenfalls erstellen/anpassen (*Auftragsbearbeitungen*; bspw. IT-Dienstleister wie Cloud-Anbieter)
- *Auslandtransfers* prüfen und allenfalls Massnahmen umsetzen (bspw. bei Cloud-Anwendungen)

Was sollten Sie wissen?

Nachfolgend konzentrieren wir uns auf: Was müssen Sie tun?

Insbesondere

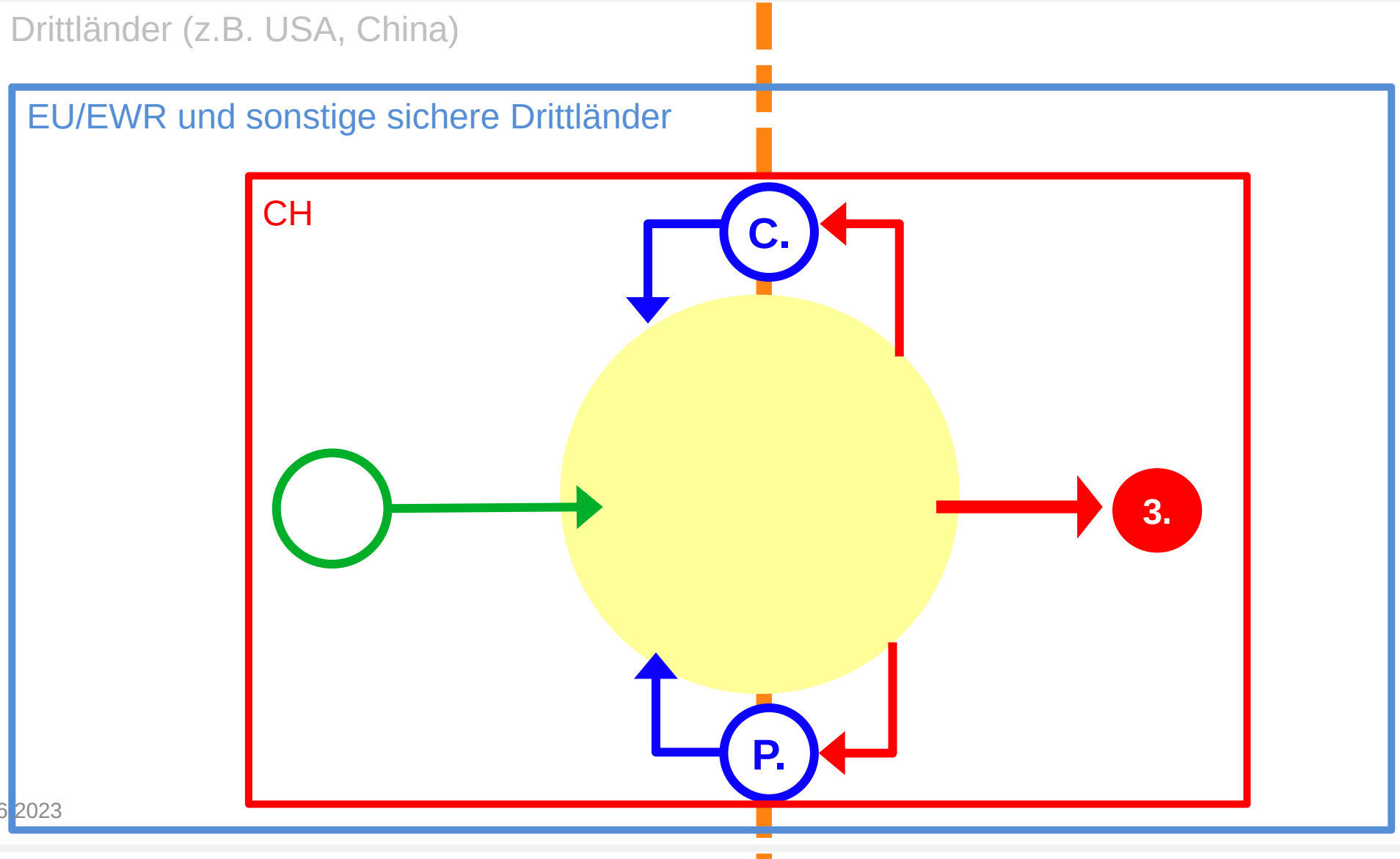
- *Datensicherheit* prüfen und allenfalls Massnahmen ergreifen
- *Datenschutz-Folgenabschätzungen* sofern erforderlich (hierauf können wir heute nicht eingehen)
- Sensibilisierung und Organisation bspw. Prozesse betr.
  - Betroffenenrechte wie Auskunft, Datenherausgabe und –übertragung
  - Meldung von Verletzungen der Datensicherheit
  - Löschung/Anonymisierung

Auswahl von Pflichten und ersten Massnahmen

Erstellen Bearbeitungsverzeichnis (Art. 12 DSG/Art. 24 DSV)

Kenntnis der Bearbeitungen

Was müssen Sie wissen?
Wie bearbeiten Sie Personendaten?



Was müssen/sollten Sie tun? - Verzeichnis

Pflicht zum Führen eines Verzeichnisses der Bearbeitungstätigkeiten

- durch Verantwortliche
- durch Auftragsbearbeiter

Ausnahme: für Unternehmen mit weniger als 250 MA, sofern
(Art. 24 DSV)

- besonders schützenswerte Personendaten nicht in grossem Umfang bearbeitet werden
- kein Profiling mit hohem Risiko durchgeführt wird

Was müussen/sollten Sie tun? - Verzeichnis

- Wichtiges Instrument für Datenschutz *auch falls im konkreten Fall keine Pflicht besteht*

- **Inhalt** des Verzeichnisses des Verantwortlichen (mindestens):
  - Identität des Verantwortlichen
  - Zweck
  - Kategorien von Betroffenen, Personendaten und Empfängern
  - Aufbewahrungsdauer oder Kriterien
  - Beschreibung Massnahmen Datensicherheit
  - Bei Bekanntgabe ins Ausland: Zielland sowie Garantien

PROBSTPARTNER

Was müssen/sollten Sie tun? - Verzeichnis

Auszug aus Beispiel

Bearbeitungstätigkeit	Zwecke der Bearbeitung	Kategorien der Personendaten	besonders schützenswerte Personendaten	Kategorien der betroffenen Personen	Herkunft der Daten	Kategorien der Empfänger	Aufbewahrungsdauer oder Kriterien zu deren Festlegung	Gewährleistung der Datensicherheit	bei Auslandtransfer: Zielländer und Garantien	Bemerkungen
(...)	(...)	(...)	(...)	(...)	(...)	(...)	(...)	(...)	(...)	
Personal										
Personaladministration	Durchführung Arbeitsverhältnis	Name und Vorname, Adresse, E-Mailadresse, AHV-Nummer, Lohn, Beschäftigungsgrad, Geburtsdatum, Familie, Zivilstand, Geschlecht, Nationalität/Heimatort, Aufenthaltsbewilligung, Kontoangaben, Eintritts-/ Austrittsdatum, Ausbildung, Berufliche Funktion, Beurteilungen, Zeiterfassung, Zugriffsrechte IT.	Gesundheitsdaten (Daten betr. Krankentaggelder, Arztzeugnisse, behinderungsbedingte Arbeitsplatzanpassungen); Daten betr. Religion (bei Abrechnung Quellensteuer)	Mitarbeiter; Angehörige Mitarbeiter (Notfallkontakte, Versicherungsleistungen)	Mitarbeiter; Muster AG; Dritte (z.B. Referenzen)	Auftragsbearbeiter (IT-Provider und Saläradministration); Behörden; Neue Arbeitgeber (Referenzauskünfte)	längstens 10 Jahre nach Beendigung Arbeitsverhältnis	siehe Datensicherheitskonzept Muster AG	Deutschland (sicheres Drittland)	
Bewerbungen	(...)	(...)	(...)	(...)	(...)	(...)	(...)	(...)	(...)	
Ehemalige Mitarbeiter	(...)	(...)	(...)	(...)	(...)	(...)	(...)	(...)	(...)	
Newsletter										
...										
Lieferantenmanagement										

strafbar

Erfüllen der Informationspflicht (Art. 19 DSG/Art. 13 DSV)

Datenschutzerklärung(en)

Erfüllen der Informationspflicht

- **Generelle Informationspflicht** bei «Beschaffung»
- Verbesserung der **Transparenz** als Grundgedanke
- **Datenschutzerklärung** gewinnt als Mittel zur Erfüllung der Informationspflicht an Wichtigkeit
- **Form**
  - «*angemessene Information*» «in *präziser, transparenter, verständlicher und leicht zugänglicher* Form» (Art. 13 DSV)
  - Erfolgt oftmals auf der Webseite
  - Zumutbare Möglichkeit zur Kenntnisnahme

PROBSTPARTNER

Erfüllen der Informationspflicht

- Kenntnis der Bearbeitungen (bspw. Verzeichnis der Bearbeitungstätigkeiten) als **Grundlage** zur Erstellung einer Datenschutzerklärung
  - Datenschutzerklärung lässt sich ohne Kenntnis der Bearbeitungen nicht korrekt, vollständig und aktuell erstellen
- Muss fortlaufend **aktualisiert** werden
- Gibt unzählige «Muster» und «Generatoren» für Datenschutzerklärungen
  - aber Achtung: die Datenschutzerklärung muss für den **Einzelfall** passen

Was müssen Sie tun? – Erfüllen der Informationspflicht

- **Mindestinhalt** der Information gemäss Art. 19 Abs. 2 DSG
  - Identität und Kontaktdaten Verantwortlicher
  - Bearbeitungszweck
  - Konkrete Empfänger oder Kategorie der Empfänger (falls vorhanden)
  - Bei Beschaffung via Dritte: Kategorien der Personendaten
  - Auslandtransfer: Garantien und konkretes (!) Zielland
  - Hinweis auf DS-Berater gemäss Art. 10 oder auf Vertretung gemäss Art. 14 DSG

- Oft enthalten, obschon nicht in Art. 19 DSG genannt: Aufklärung über Rechte, wie
  - Auskunft, Berichtigung, Löschung oder Vernichtung, Datenherausgabe oder -übertragung
  - Widerruf einer allfälligen Einwilligung
  - Beschwerde beim EDÖB

- Inhalte, die in manchen DSE enthalten, aber unüblich sind:
  - Rechtsgrundlage
  - Aufbewahrungsdauer
  - Herkunftsangaben

strafbar

Verträge prüfen und allenfalls erstellen/anpassen

Auftragsbearbeitung (Art. 9 DSG)

Was müssen Sie tun? – Auftragsbearbeitungen

Worum geht es?

- So genannte „Auftragsbearbeitungen“

Wann liegt eine Auftragsbearbeitung vor?

- «Verantwortlicher» vs. «Auftragsbearbeiter»

- Beispiele:
  - IT-Dienstleister?
  - Cloud-Anbieter?
  - Auslagerung Lohnadministration?

Was müssen Sie tun? – Auftragsbearbeitungen

- Zulässig, wenn
  - Übertragung durch Vertrag (oder Gesetz) erfolgt
  - Auftragnehmer Daten bearbeitet wie Verantwortlicher
  - Keine Geheimhaltungspflicht entgegensteht
  - Datensicherheit gewährleistet ist (regelmässige Kontrolle)
  - Unterauftragnehmer nur mit Genehmigung des Verantwortlichen

- Vorgehen
  - Wo werden Dritte beigezogen? Prüfen …
  - Sind diese Auftragsbearbeiter?
  - Überprüfen, ob/welche Verträge bereits bestehen und ob weitere Voraussetzungen erfüllt
  - Verträge gemäss neuen Anforderungen aktualisieren und dokumentieren
  - Wo noch keine (schriftlichen) Verträge: erstellen und dokumentieren

- PS:
  - Meldung bei Datenschutzverletzungen und Unterstützung bspw. bei Erteilung Auskunft vertraglich verankern (inkl. Regelung zur Kostentragung)

PROBSTPARTNER

Bekanntgabe ins Ausland (Art. 16 f. DSG)

strafbar

Prüfen und allenfalls Massnahmen umsetzen

Was müssen Sie tun? – Bekanntgabe in Ausland

- Bekanntgabe ist «Übermitteln oder Zugänglichmachen»
- Bspw. bei Dienstleistern im Ausland / Cloud
- Unterscheiden «sicheres» und «unsicheres» Ausland
- Bekanntgabe in «sicheres» Ausland ohne weiteres möglich
- In «unsicheres» Ausland Bekanntgabe nur mit zusätzlichen Schutzmassnahmen, wie bspw.
  - Standarddatenschutzklauseln mit Anpassungen und Transfer Impact Assessment
  - Einwilligung (oftmals nicht praktikabel)

Was müssen Sie tun? – Bekanntgabe in Ausland

- Bekanntgabe in «unsicheres» Ausland mit hohem Aufwand verbunden
  - Gibt es Alternativen?
  - Gibt es Anbieter mit Sitz in der Schweiz/EU/EWR?
  - Serverstandort in der Schweiz/EU/EWR wählen …

strafbar

Vorschriften betr. Datensicherheit (Art. 8 DSG/Art. 1 ff. DSV)

Was müssen Sie tun? – Datensicherheit

«Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine **dem Risiko angemessene** Datensicherheit.» (Art. 8 Abs. 1 DSG)

Mindestanforderungen in DSV:

- Risikobasierter Ansatz, u.a. potentielle Auswirkungen, Stand der Technik, Kosten
- Technische und organisatorische Massnahmen zum Schutz:
  - Vertraulichkeit
  - Verfügbarkeit
  - Integrität
  - Nachvollziehbarkeit

In gewissen Fällen Bearbeitungsreglement und/oder Protokollierungspflicht

PROBSTPARTNER

Was müssen Sie tun? – Datensicherheit

Meldepflicht von Verletzungen der Datensicherheit (Art. 24 DSG / Art. 15 DSV)

- an EDÖB, wenn voraussichtlich zu hohem Risiko für die betroffene Person führt
- so rasch als möglich (vs DSGVO: 72 Stunden)
- an betroffene Person, wenn zu ihrem Schutz erforderlich oder EDÖB verlangt

Zu tun:

- Prüfen, anpassen von technischen und organisatorischen Massnahmen
- Prüfen und gegebenenfalls umsetzen Protokollierung / Bearbeitungsreglement
- Einführen von Prozessen für Aufnahme neuer Bearbeitungstätigkeiten und für Datensicherheitsvorfälle
- Lassen Sie sich beraten …

Weiteres

Was müssen Sie tun? – Weiteres

Weitere To-Dos

- *Datenschutz-Folgenabschätzungen* sofern erforderlich (hierauf können wir heute nicht eingehen)

- Sensibilisierung und Organisation bspw. Prozesse betr.
  - Betroffenenrechte wie Auskunft, Datenherausgabe und –übertragung
  - Meldung von Verletzungen der Datensicherheit
  - Löschung/Anonymisierung

- Weiteres mehr

Wo gibt es weitere Informationen?

PROBSTPARTNER

Wo gibt es weitere Informationen?

- **EDÖB:**

  https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/grundlagen/ndsg.html

- Diverse Websites

- Diverse Kurse und Workshops

Die Umsetzung braucht zwar Zeit, ist aber machbar: Beginnen Sie einfach damit!

Herzlichen Dank für Ihre Aufmerksamkeit!

Dr. iur. Michael Widmer, LL.M.
Rechtsanwalt
michael.widmer@probstpartner.ch

Probst Partner AG, Zürich/Winterthur
+41 52 269 1400
www.probstpartner.ch