DSGVO – Inwiefern weicht der Entwurf DSG-CH davon ab? (ohne Behördenverkehr)

RA Dr. Christian Laux, LL.M.

LAUX LAWYERS AG
ZURICH | BASEL

DGRI – Drei-Länder-Treffen

St. Gallen

23. Juni 2018

Warum interessiert «uns» das?

LAUX LAWYERS AG
ZURICH | BASEL

- Wird die EU die Äquivalenz der Schweizer Datenschutz-Gesetzgebung weiterhin anerkennen?
- Der Schweizerische Bundesrat meint:

  Die Beibehaltung des Angemessenheitsbeschlusses der EU ist für den Bundesrat ein vorrangiges Ziel. Namentlich aus diesem Grund hat er beschlossen, den Inhalt des E-DSG den Anforderungen des Entwurfs zur Revision des Übereinkommens SEV 108 und der DSGVO anzugleichen.

  Wann die Europäische Kommission die Angemessenheit des schweizerischen Datenschutzrechts erneut überprüfen und ob das Resultat positiv ausfallen wird, ist heute nicht vorhersehbar. Damit die Schweiz die bestehende Angemessenheitserklärung beibehalten kann, muss sie ein vergleichbares Schutzniveau aufweisen wie die EU.

  Der Ausgang der Prüfung hängt wesentlich von den Entscheidungen des Parlaments im Rahmen der Revision der schweizerischen Datenschutzgesetzgebung ab.

Vergleichswerte

	DSGVO	DSG-CH (Entwurf)
Umfang (Seiten)	• Recitals: 31 Seiten • Verordnungstext: 57 Seiten • Weitere Anpassung EU: ePrivacy • Anpassungsgesetze: pro Land	• Recitals: 0 Seiten • Gesetzestext: 28 Seiten • Weitere Anpassungen: 52 Seiten • Kantone: pro Kanton
Umfang (Artikel)	99 Artikel	67 Artikel

Vergleichswerte

	DSGVO	DSG-CH (Entwurf)
Gesetzgebungsverfahren (1/2)	abgeschlossen	Tranche 1 (Schengen): • Erstrat: Sommer ‘18 / Herbst ‘18 • Zweitrat: Herbst ‘18 / Frühj. ’19 • eventuell: Differenzbereinigung • Abstimmung nach Referendum (?)
Gesetzgebungsverfahren (2/2)	n.a.	Tranche 2 (Totalrevision): • Erstrat: Frühjahr ‘19 / Sommer ‘19 • Zweitrat: Sommer ‘19 / Herbst ‘19 • Eventuell: Differenzbereinigung • Abstimmung nach Referendum (?)
Inkrafttreten	25. Mai 2018	Tranche 1: nicht vor Sommer 2019 Tranche 2: nicht vor April 2020

Differenzierungen

	DSGVO	DSG-CH (Entwurf)
Sonderregeln für Behörden	Ja	Ja
Sektorspezifische Regeln	Nein	Am Rande (Bonitätsdaten, etc.)

Anwendungsbereich

	DSGVO	DSG-CH (Entwurf)
Örtlicher	Kriterium des Personenbezugs Kriterium des EU-Bezugs	Kriterium des Personenbezugs Begehung/Erfolg in CH oder Binnensachverhalt
Sachlicher	• Speicherung in Dateisystem oder • zumindest teilautomatisierte Verarbeitung	• umfassend

Umsetzungsfragen DSGVO im Verhältnis zur Schweiz

LAUX LAWYERS AG
ZURICH | BASEL

- Sind Schweizer Unternehmen der DSGVO unterstellt?
  - Das kann vorkommen.
- Welche Aufsichtsbehörde ist dann für das Unternehmen zuständig?
  - Auswirkungsprinzip
- Die DSGVO verweist an vielen Stellen auf das Recht der Mitgliedsstaaten. Welche Rolle spielt dabei das schweizerische Recht?
  - Die Schweiz ist kein Mitgliedstaat im Sinn der DSGVO. Die Verweisungen auf das Recht der Mitgliedstaaten umfassen das schweizerische Recht nicht, welchem folglich auch keine Rolle zukommt.

Umsetzungsfragen DSGVO im Verhältnis zur Schweiz

- Lässt sich die DSGVO in der Schweiz durchsetzen?

  Der Schweizerische Bundesrat meint dazu:

  Die Untersuchung und die Verhängung von Sanktionen gegen ein Unternehmen mit Sitz in der Schweiz, das aber der DSGVO unterstellt ist, fallen in die Zuständigkeit der Aufsichtsbehörden der EU-Mitgliedstaaten.

  ***Ohne ein Kooperationsabkommen können diese jedoch selbst keine Untersuchungshandlungen in der Schweiz durchführen**.*

  Muss ein Unternehmen einen Vertreter in der EU benennen (Art. 27 DSGVO), können die europäischen Aufsichtsbehörden ihre Entscheidungen dem schweizerischen Unternehmen über diesen Vertreter zustellen, ohne den diplomatischen Weg zu beschreiten.

- **ÄTSCH!** (aber faktisch: CH-Unternehmen werden oft auch sonstige Assets in der EU belegen haben, was trotzdem Rechtsdurchsetzungsmassnahmen in der EU eröffnet – Konfiskation im Widerhandlungsfall ...)

Umgekehrt: Werden CH-Standards anerkannt?

- Werden Schweizer Zertifizierungen und Zertifizierungsstellen von der EU anerkannt?
  - Nein (derzeit nicht vorgesehen)

Bilateraler Weg?

- Der Schweizerische Bundesrat will zuwarten
- Dass die Sache eskaliert und «verpolitisiert» wird, ist nicht auszuschliessen

Gegenüberstellung High Level

Gegenüberstellungen (1/2)

- Grosse Unterschiede:
  - Sanktionenkonzept
  - Herausgabeansprüche (insb. Datenportabilität)
  - Datenschutzberater («DSB») fakultativ
  - Rechte verstorbener Personen
- Dann: eine Vielzahl von kleineren Abweichungen, die:
  - Unternehmen das Leben etwas schwer machen
  - ... bzw. jedenfalls **teurer**

Gegenüberstellungen (2/2)

- Was ist im Wesentlichen identisch?
- Datenschutzgrundsätze
- Privacy by Design / by Default
- Auftragsdatenverarbeitung
- Diverse Betroffenenrechte:
  - Berichtigung
  - Einschränkung der Verarbeitung
  - Löschung
  - Information bei AEFE
  - Anhörung bei AEFE

Grundprinzipien

	DSGVO	DSG-CH (Entwurf)
Rechtmässigkeitsvorbehalt (*für andere als besondere Kategorien von personenbezogenen Daten*)	**Ja**: «Die Verarbeitung ist **nur rechtmäßig**, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:» • [**Einwilligung**], [**Vertrag**], • **[berechtigte Interessen]**, • [**Gesetz**], etc.	**(na) Ja** («moderater Vorbehalt»): «Wer Personendaten bearbeitet, darf die **Persönlichkeit** der betroffenen Personen **nicht widerrechtlich verletzen***.» «Eine Persönlichkeitsverletzung ist widerrechtlich, wenn sie nicht [gerechtfertigt ist] durch **Einwilligung** der betroffenen Person, durch ein **überwiegendes [...] Interesse** oder durch **Gesetz**

* **Persönlichkeitsverletzung**: (2) Eine Persönlichkeitsverletzung liegt insbesondere vor, wenn: a. Personendaten entgegen den [**Grundsätzen**: Datenverarbeitungsgrundsätze, Privacy by Design, Privacy by Default, Datensicherheit] bearbeitet werden; b. Personendaten **entgegen der ausdrücklichen Willenserklärung** der betroffenen Person bearbeitet werden; .... (3) [Aber nicht: Wenn öffentlich gemacht]

Grundprinzipien

	DSGVO	DSG-CH (Entwurf)
Rechtmässigkeitsvorbehalt (*für besondere Kategorien von personenbezogenen Daten*)	**Ja**: «Die Verarbeitung [von beso. Kategorien personenbezogener Daten] … ist untersagt») • Absatz 1 gilt nicht in folgenden Fällen: [enger umschriebene Rechtfertigungsgründe]	**(na) Ja** («moderater Vorbehalt»): «Wer Personendaten bearbeitet, darf die **Persönlichkeit** der betroffenen Personen **nicht widerrechtlich verletzen***.» «Eine Persönlichkeitsverletzung ist widerrechtlich, wenn sie nicht [gerechtfertigt ist] durch **Einwilligung** der betroffenen Person, durch ein **überwiegendes [...] Interesse** oder durch **Gesetz**

* **Persönlichkeitsverletzung**: (2) Eine Persönlichkeitsverletzung liegt insbesondere vor, wenn: a. Personendaten entgegen den [**Grundsätzen**: Datenverarbeitungsgrundsätze, Privacy by Design, Privacy by Default, Datensicherheit] bearbeitet werden; b. Personendaten **entgegen der ausdrücklichen Willenserklärung** der betroffenen Person bearbeitet werden; c. **Dritten besonders schützenswerte Personendaten bekanntgegeben** werden. (3) [Aber nicht: Wenn öffentlich gemacht]

Auswahl der Themen: Weitgehend kongruent

Massnahmen (Basis)

Minimum

Verfahrensverzeichnis
EU: +250 // CH: (-50)

Dokumentation

Massnahmen (stützend)

Measures

Technische Massnahmen

Organisatorische Massnahmen

Vertragliche Massnahmen

Policies & Code of Conduct

Massnahmen (situativ)

Standard

Massnahmen zur Rechtfertigung (Art. 6 – 11)

Sicherheitsvorfälle (Art. 33 und 34)

Transparenzmeldungen (Art. 12 – 14)

DSFA (Art. 35)

Betroffenenrechte (Art. 15 – 23)

Grenzüberschreitend (Art. 44 ff.)

Beschäftigte

Kontrolle über DL (ADV) (Art. 28)

Deutlich anders: Sanktionenkonzept

	DSGVO	DSG-CH (Entwurf)
Wie wird sanktioniert?	Geldbusse oder Zwang	• Geldbusse bis CHF 250'000 • Alternatives Vorgehen bei Bussen bis zu CHF 50'000
Wer wird sanktioniert?	Unternehmen	• Privatperson • Subsidiär: Unternehmen

Sanktionenkonzept

Der Bundesrat meint dazu:

1. [Der Bundesrat] ist der Ansicht, dass die Einführung solcher Sanktionen im DSG nicht angemessen ist, denn **Verwaltungsstrafen**, die Sanktionscharakter haben, **müssen die Ausnahme** und auf Sektoren beschränkt bleiben, in denen die Zielgruppe beschränkt ist (namentlich Kartelle, Geldspiele). Mangels spezifisch auf solche Sanktionen anwendbarer Verfahrensgrundsätze besteht die Gefahr, dass die Verfahrensgarantien zum Schutz der fehlbaren Personen verletzt werden.
2. Es besteht **kein Grund zur Befürchtung**, **dass jede Angestellte oder jeder Angestellte** eines Unternehmens, das Personendaten bearbeitet, bestraft werden könnte. Die Mehrheit der strafbaren Verhaltensweisen betreffen den Verantwortlichen. Handelt es sich dabei um eine juristische Person, wird die Straftat gemäss Artikel 29 StGB der Vertreterin oder dem Vertreter des Geschäftsorgans zugerechnet.

Sanktionen

- Die Einhaltung des Schweizerischen Rechts begründet nicht zugleich auch die Einhaltung der DSGVO
- Können Unternehmen für den gleichen Fall sowohl von der Schweiz, als auch von Seiten EU sanktioniert werden?
  - Das könnte vorkommen
- Der Schweizerische Bundesrat meint dazu:

  «Der Grundsatz ne bis in idem (Verbot der doppelten Strafverfolgung) könnte jedoch zur Anwendung kommen, wenn Geldbussen der EU und strafrechtliche Sanktionen der Schweizer Strafverfolgungsbehörden zusammentreffen.»

Würdigung

- Wir stellen fest:
  - Leicht anderes Rechtfertigungsmodell
  - ... bei gleichbleibenden Compliance ToDo's
  - ... und verschärftem Sanktionenkonzept ...
- ... führt zu Folgendem:
  - Compliance-«Übungen» und entsprechenden Kosten
  - Für KMU nicht unbedingt vorteilhafte Situation

Gegenüberstellung im Einzelnen

Identisch: Auftragsdatenverarbeitung

	DSGVO	DSG-CH (Entwurf)
Zulässig bei «normalen» pb Daten	Ja	Ja
Zulässig bei bes. Kat. pb Daten	Ja	Ja
Zustimmung der betroffenen Person	Nicht erforderlich	Nicht erforderlich
Meldung an die betroffene Person	str. (wenn ja: ohne Details)	str. (wenn ja: ohne Details)
Beizug von Subprocessors	• generelle Genehmigung genügt (erfordert aber Meldung), sonst • Zustimmung im Einzelfall	• generelle Genehmigung genügt (erfordert aber Meldung), sonst • Zustimmung im Einzelfall
Abgeleitete Befugnis	Verarbeitung wie Controller zulässig, im Rahmen von dessen Instruktion	Verarbeitung wie Controller zulässig, im Rahmen von dessen Instruktion

für eine harmonisiert vereinfachte Darstellung siehe: https://cloudprivacycheck.eu/

Etwas anders: Einwilligung

	DSGVO	DSG-CH (Entwurf)
Freiwilligkeitserfordernis	Ja	Ja
Informationspflicht vorab	Ja Wenn schriftliche Korrespondenz: • verständlich • leicht zugänglich • klar • einfach formuliert • getrennt erfolgen	Ja («angemessene» Information)
Eindeutigkeit bei Einwilligungen	Nicht explizit verlangt	**Generell verlangt**
Ausdrücklichkeit bei Einwilligungen	Nicht explizit verlangt	**Verlangt für bes. Kat. pbD / Profiling / AEFE**

Etwas anders: Betroffenenrechte

	DSGVO	DSG-CH (Entwurf)
Information bei Erhebung von Daten «an der Quelle»	Ja, proaktiv / voraussetzungslos	Ja, proaktiv / voraussetzungslos (**aber per Generalklausel …**)
Information bei Erhebung von Daten bei Dritten	Ja, proaktiv / voraussetzungslos	Ja, proaktiv / voraussetzungslos (**Nennung Herkunft nur auf Anfrage**)
Information bei AEFE	Ja	Ja, wenn «Rechtsfolge» oder «erhebliche Beeinträchtigung», **ausser** • AEFE nötig für Vertrag und fällt aus wie gewünscht (von betr. P.) • ausdrückl. Einwilligung
Anhörung	Ja, AEFE	Ja, AEFE

Deutlich anders: Herausgaberechte

	DSGVO	DSG-CH (Entwurf)
Auskunft (abstrakte Information)	Ja	Ja (**aber per Generalklausel …**)
Herausgabe («als PDF»)	Ja (Art. 15(3)), Freiheitsrechte Dritter vorbehalten	**Nein** (ist heute aber gelebte Praxis)
Datenportabilität	Ja (für Daten, die betr. Person mitgeteilt hat; automat. verarbeitet; auf Basis Vertrag / Zustimmung)	**Nein**

Deutlich anders: Betroffenenrechte

	DSGVO	DSG-CH (Entwurf)
Berichtigung	Ja	Ja
Einschränkung der Verarbeitung	Ja	Ja
Löschung	Ja	Ja
Löschdurchsetzung bei Dritten	Ja	**Nein**

Immer wieder anders: Betroffenenrechte

	DSGVO	DSG-CH (Entwurf)
Widerspruch gegen Verarbeitung	Ja: • bei Direktmarketing: voraussetzungslos • sonst eingeschränkt: abhängig von Interessenabwägung	Ja: • bei Direktmarketing: **abhängig von Interessenabwägung** • sonst eingeschränkt: abhängig von Interessenabwägung
Keine AEFE	AEFE sind erlaubt, wenn: • Sicherheitsmassnahmen • Anhörungsrecht … umgesetzt sind	AEFE sind erlaubt. Sicherheitsmassnahmen und Anhörung **sind** auch umzusetzen, **aber nicht konditional**.
«Rechte Verstorbener»	Keine	**Einsichts- und Löschrechte**

Deutlich anders: «Datenschutzbeauftragter»

LAUX LAWYERS AG
ZURICH | BASEL

	DSGVO	DSG-CH (Entwurf)
Bezeichnung	Datenschutzbeauftragter	Datenschutzberater
Kann-Regelung	Nein (ersatzweise ja, 37(4))	Ja
Notwendig für Private, wenn **Kerntätigkeit** Folgendes umfasst:	• Überwachung (umfangreich, regelmässig, systematisch) • umfangreiche Bearbeitung von bes. Kateg. von pb Daten	**keine Notwendigkeit** (aber Voraussetzung für **Rechtsfolgenbefreiung**, s.u.)
Sonstwie notwendig für Private:	Nach Landesrecht (z.B. D: 10 MA)	**n.a.**
Notwendig für Behörden, wenn …:	voraussetzungslos (nicht rechtsprechende Behörden)	keine Notwendigkeit (aber Voraussetzung für Rechtsfolgenbefreiung, s.u.)
Rechtsfolgenbefreiung	keine	Keine Pflicht zur Einholung einer Stellungnahme der Behörde für DSFA

Etwas anders:
Datenschutzfolgeabschätzung

	DSGVO	DSG-CH (Entwurf)
Voraussetzungen	Ja, wenn: • hohes Risiko Beispiele: • AEFE • Verarbeitung von bes. Kat. pbD «at a large scale» • Systematisches Monitoring von öffentlichen Bereichen	Ja: • bei «hohen Risiken» • **bei Profiling: immer** Reaktion EDÖB: 3 Monate

Etwas anders:
Meldung «Data Breach»

	DSGVO	DSG-CH (Entwurf)
Anlassfall (erste Stufe)	• Verletzung des Schutzes pbD • es resultiert ein Risiko	• Verletzung der Datensicherheit • es resultiert ein **hohes** Risiko
Meldung an wen?	• Aufsichtsbehörde • innert 72 Stunden	• Aufsichtsbehörde • rasch
Anlassfall (zweite Stufe)	• es resultiert voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen	• wenn erforderlich zum Schutz der betroffenen Person • wenn die Aufsichtsbehörde es verlangt
Meldung an wen?	• Betroffene Person • anschliessend	• Betroffene Person • **rasch (auch zeitgleich?)**

Etwas anders:
Datenschutz und Technik

	DSGVO	DSG-CH (Entwurf)
Privacy by Design	Ja	Ja
Privacy by Default	Ja	Ja
Pflicht zur Datensicherheit	Ja, «[MN] schliessen … ein»: Pseudonymisierung, Verschlüsselung, CIA+Belastbarkeit, Recovery, Review	Ja, Zielvorgabe: • Datenschutzgrundsätze einhalten • Eignung, vor Breach zu schützen

Kontakt

Dr. Christian Laux
Rechtsanwalt
christian.laux@lauxlawyers.ch

LAUX LAWYERS AG
http://www.lauxlawyers.ch

Seegartenstrasse 2
Postfach 360
CH – 8024 Zurich
+41 44 880 24 24