LAUX LAWYERS AG
ZURICH | BASEL

BÜRO ZÜRICH
Seegartenstrasse 2
P. O. Box 360 · CH 8024 Zürich
T +41 44 880 2424
F +41 44 880 2425
W www.lauxlawyers.ch

BÜRO BASEL
Steinenring 40 · CH 4051 Basel
T +41 61 283 0606
W www.lauxlawyers.ch

RECHTSANWÄLTE
Z Dr. Christian Laux · LLM
Z Dr. Jürg Hess · MBA · M.C.J.
Z Alexander Hofmann
B Mark Schieweck

In den zuständigen Anwaltsregistern eingetragen

P.O. Box 360, CH 8024 Zürich

per Email zu Handen: jonas.amstutz@bj.admin.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundeshaus West
3003 Bern

4. April 2017

Stellungnahme zum Vorentwurf zur Totalrevision des Datenschutzgesetzes

Sehr geehrte Frau Bundesrätin,
Sehr geehrte Damen und Herren

LAUX LAWYERS AG ist eine Anwaltskanzlei mit Fokus IT-Recht. Unsere Aufgabe sehen wir darin, durch spezialisierte Fachkompetenz an der Schnittstelle zwischen Recht und IT den IT-Sektor zu unterstützen. Mit dieser Aufgabenstellung beraten wir unter anderem sowohl Kunden und Nutzer von Outsourcings als auch Anbieter von solchen Leistungen (kundenindividuelle Auslagerungen, Cloud Computing und Managed Services).

Mit dieser Eingabe nehmen wir Stellung zur Vernehmlassungsvorlage betreffend Totalrevision des Datenschutzgesetzes (VE-DSG, gemäss Mitteilung des Bundesrats vom 21. Dezember 2016).

Wir erlauben uns, in Bezug auf die in Anhang 1 kommentierten Bestimmungen des VE-DSG zu schildern, inwiefern diese die Digitalisierungsbestrebungen in der Schweiz beeinträchtigen würden. Dabei beschränken wir uns auf Kommentare zum eingangs erwähnten „Cloud Computing". Wir hoffen, mit diesem fokussierten Beitrag die Diskussion zum VE-DSG bereichern zu können.

A. Zum Cloud Computing und seiner Bedeutung für den Datenschutz

1 Cloud Computing ist ein Sammelbegriff für technische IT-Infrastrukturen, die zusammen mit ergänzenden Dienstleistungen für die Digitalisierung der Schweiz von grösster Bedeutung sind. Das massgebliche Merkmal solcher Dienstleistungen besteht darin, dass dank standardisierter Technologie sowie standardisierten, ergänzend bereitgestellten Dienstleistungen vermehrt softwareunterstützte Prozesse zur Verfügung stehen oder abgebildet werden können, für die ein Kunde zuvor ungleich grössere finanzielle Mittel hätte aufwerfen müssen.

2 Dies bedingt, dass der Cloud-Anbieter sich für eine Vielzahl von Kunden so organisiert, dass er gleichartige IT-Infrastrukturen und gleichartige Prozesse allen Kunden unterschiedslos zur Verfügung stellen kann. Der Anbieter sorgt mittels technischer, organisatorischer und vertraglicher Massnahmen dafür, dass seine eigenen Mitarbeitenden nicht auf Daten von Kunden Zugriff nehmen und dass einzelne Kunden nicht auf Daten von anderen Kunden Zugriff nehmen können.

3 Je nach Situation und der vom Anbieter gewährten Transparenz kann der Kunde die vom Cloud-Anbieter getroffenen technischen und organisatorischen Massnahmen direkt nachvollziehen. Zusätzlich sichert der Cloud-Kunde seine Schutzziele – Schutz vor unbefugtem Zugriff, Schutz vor unbefugter Verwertung und Integritäts- sowie Verfügbarkeitsschutz – vertraglich ab. Dabei unterscheiden sich Cloud-Angebote für die Geschäftsnutzung erheblich von Angeboten, die sich an den Endkunden (Konsumenten) richten.

4 Erscheinungsformen:

> ***IaaS**: Ein Kunde verwaltet nicht mehr wie bis anhin eigene Hardware und Plattformsoftwares, um anschliessend Applikationen zur eigenen Nutzung zu installieren. sondern wird vom Cloud-Anbieter im Resultat gleichgestellt, indem dem Kunden sog. Virtuelle Server („Virtual Machines") zur Verfügung gestellt werden. Der Cloud-Anbieter setzt aber zu diesem Zweck IT-Infrastrukturen ein. zu deren Schutz er die technisch und organisatorisch relevanten Massnahmen ergreift. Man spricht hier von Infrastructure as a Service (oder IaaS). weil dem Kunden die Aufgabe abgenommen wird, selber den Standort des Servers zu bestimmen. die Hardware auszuwählen und lauffähig zu erhalten. Der Kunde bleibt aber in der Verantwortung. die Virtuelle Maschine so mit Betriebssystemen auszustatten. dass sie für ihn nützlich ist. Einblick des Cloud-Anbieters in die Virtuelle Maschine (und damit Einsicht in Daten) ist technisch nicht erforderlich, dass das IaaS-Angebot dem Kunden nützlich ist.*
>
> ***PaaS**: Wenn der Cloud-Dienstleister dem Kunden darüber hinaus weitere Verwaltungstätigkeiten abnimmt (gleich wie zuvor der IT-Dienstleister, der dem Kunden über Remote-Zugriff von aussen geholfen hat, Betriebssysteme. Datenbanken und dergleichen in Stand zu halten), spricht man von Platform as a Service (PaaS). Der Kunde kann sich darauf beschränken, die für ihn relevanten Applikationen aufzusetzen, so dass sie ihm nützlich sind. Cloud-Anbieter, die nach modernen Verfahren organisiert sind. erbringen die Verwaltungstätigkeiten zum Betrieb der Plattformsoftwares mit Hilfe von automatisierten Prozessen und müssen entsprechend keinen kundenspezifischen Einblick in Daten von Kunden erhalten, um den Service anbieten zu können.*
>
> ***SaaS**: Ähnlich wie im PaaS-Konzept stellt der SaaS-Anbieter (SaaS für „Software as a Service") direkt nutzbare Software zur Verfügung. Der Cloud-Anbieter hat im SaaS-Modell die vom Kunden genutzte Applikation allerdings bereits vorinstalliert und nutzbar gemacht. Der Kunde kann sich darauf beschränken, die Applikation zu bedienen; allenfalls kann er sie anhand von vorhandenen Parametern auf seine Bedürfnisse einstellen.*

5 Beispiele für Cloud-Angebote, die sich an Geschäftskunden richten:

> ***IaaS**: Ein Unternehmen bezieht reine IT-Infrastrukturleistungen vom Anbieter, betreibt die darauf zu installierende Betriebssystemsoftware und Applikationen aber selber / durch eigenes Personal.*
>
> ***SaaS**: Ein Unternehmen bezieht eine Applikation zur Arbeitszeitenerfassung und zur Verwaltung weiterer Personalfragen über einen Dienstleister. Die inhaltliche Bearbeitung nimmt allein das Unternehmen vor.*

6 Beispiel für Cloud-Angebote, die sich an Konsumenten richten:

> ***SaaS**: Ein Konsument benutzt einen Cloud-Dienst, um seine Fotos an zentraler Stelle abzulegen.*

B. Relevante Bestimmungen im VE-DSG aus Kundensicht

7 Aus Kundensicht stellen sich gemeinhin vier wesentliche Kernfragen, die unter anderem unter http://www.cloudprivacycheck.eu schematisch und übersichtlich dargestellt sind:

- Daten unter Dritteinfluss: Sind Datenschutzaspekte zu beachten, weil der Cloud-Kunde Daten bearbeitet, in Bezug auf welche er gegenüber Dritten Rechenschaft ablegen muss?
- Beizug eines Dritten / Technische und organisatorische Massnahmen: Welche IT-Infrastrukturen betreibt der Cloud-Anbieter und welche technischen und organisatorischen Massnahmen ergreift er?
- Datenhaltung im Ausland oder Datenzugriff aus dem Ausland: Inwiefern entsteht durch die Nutzung des Cloud-Anbieters bzw. der von ihm bereitgestellten Dienste ein Auslandbezug?

- Subunternehmer: Inwiefern stellt der Cloud-Anbieter auf Subunternehmer ab?

8 Der Vorentwurf beschlägt diesen Fragekatalog wie folgt:

- Daten unter Dritteinfluss: Der Begriff der Personendaten wird enger gefasst (keine Regelung von Unternehmensdaten; insofern wird der Anwendungsbereich von Daten unter Dritteinfluss reduziert, was zu begrüssen ist). Die Regelung verbessert den Handlungsspielraum für Cloud-Kunden.

- Beizug eines Dritten / Technische und organisatorische Massnahmen: Als besonders störend ist die Regelung von Art. 13 Abs. 4 VE-DSG hervorzuheben. Die dort postulierte Mitteilungspflicht ist systemwidrig, hat keinen Mehrwert und führt wohl in aller Regel gar zu Mitteilungen, welche die betroffene Person über den tatsächlichen Schutz ihrer Personendaten in die Irre führen können.

- Datenhaltung im Ausland oder Datenzugriff aus dem Ausland: Der Beizug von Dienstleistern aus dem Ausland wird erschwert (erschwerte Planung wegen z.T. komplizierterer Regelungen).

- Subunternehmer: Würde Art. 7 Abs. 3 VE-DSG nicht „europakompatibel" gelesen werden können (nämlich: nachträgliche Meldung genügt, solange der Cloud-Anbieter generell im Vertrag ermächtigt ist, Subunternehmer beizuziehen), würde die Stellung des Cloud-Kunden auf den ersten Blick zwar verbessert; insgesamt würde die wenig hilfreiche Regelung allerdings das Leistungsangebot für Cloud-Kunden reduzieren (weil weniger Anbieter bereit wären, zu diesen Bedingungen Cloud-Angebote an Kunden in der Schweiz zu erbringen). Ein Cloud-Kunde, dem der Cloud-Anbieter Transparenz über beigezogene Dienstleister verspricht, ist auf die strengere („nicht europakompatible") Lesart aber nicht angewiesen, um Kontrolle über den Dienstleister und das Leistungsangebot auszuüben.

9 Bestimmungen, die den Cloud-Kunden einschränken, sind zu vermeiden, da sie die Digitalisierungsbestrebungen der Schweiz bremsen und die Wettbewerbsfähigkeit der Schweiz beeinträchtigen. Wir verweisen für detaillierte Kommentare hierzu auf Anhang 1 zu diesem Schreiben.

C. Relevante Bestimmungen im VE-DSG aus Anbietersicht

10 Aus Anbietersicht enthält der Vorentwurf gewisse Bestimmungen, welche die Rollenteilung zwischen Auftragsdatenbearbeiter und Verantwortlichem verwischen, ohne dass dazu ein Anlass bestünde. Zu nennen sind:

- Art. 16 VE-DSG: Datenschutzfolgeabschätzung sollte ein Cloud-Anbieter nur vornehmen müssen, wenn er Verantwortlicher ist. Ist er allein als Auftragsdatenbearbeiter tätig, trifft die Pflicht zur Datenschutzfolgeabschätzung allein den Cloud-Kunden (als Verantwortlichen).

- Art. 17 VE-DSG: Die (strafbewehrten) Pflichten, eine Data Breach Notification abzusetzen, sollten den Cloud-Anbieter (als Auftragsdatenbearbeiter) nur in der ihn betreffenden Risikosphäre treffen. Diese sollte präzisiert werden.

- Art. 18 VE-DSG: Privacy by Design sollte dem Cloud-Anbieter nicht als eigene Pflicht auferlegt werden (solange er nur als Auftragsdatenbearbeiter tätig ist); aber selbstverständlich wird der Cloud-Anbieter den Verantwortlichen bei der Umsetzung von solchen Massnahmen unterstützen müssen.

- Art. 19 lit. b VE-DSG: Die in Art. 19 lit. b VE-DSG genannten Informationspflichten könnte der Cloud-Anbieter nicht wahrnehmen, wenn er das oberste Ziel (keinen Zugriff auf Daten des Cloud-Kunden) umsetzt. Die Regelung steht insofern in grellem Kontrast zu den technischen und organisatorischen Massnahmen, die für seriöse Cloud-Anbieter als State of the Art bezeichnet werden können.

- Art. 20 Abs. 5 VE-DSG: Die Regelung würde die Attraktivität des Standorts Schweiz für Cloud-Anbieter erheblich beeinträchtigen.

11 Detaillierte Anmerkungen zu diesen Bestimmungen finden sich wiederum in Anhang 1 zu diesem Schreiben.

12 Gesamthaft lässt sich festhalten, dass der Vorentwurf den Auftragsdatenbearbeiter nicht nur als ausführende Stelle behandelt, die zur Einhaltung von Weisungen des Verantwortlichen verpflichtet ist, sondern ihn in Verkennung der Gesetzessystematik darüber hinaus als eigenständigen Risikoträger behandelt. Wir halten dies nicht für empfehlenswert. Die Rechtsbeziehung zwischen Cloud-Anbieter und Cloud-Kunde sollte abschliessend durch Art. 7 und Art. 11 VE-DSG geregelt sein.

* * *

Abschliessend bitten wir Sie höflich um positive Auseinandersetzung mit unseren Vorschlägen. Gerne stehen wir für allfällige Präzisierungen zur Verfügung. Für Ihre Bemühungen danken wir Ihnen bestens.

Freundliche Grüsse

Christian Laux Alexander Hofmann

Anhang 1: Ausformulierte Kommentierungen und Anpassungsvorschläge

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Stellungnahme von

Name / Firma / Organisation : LAUX LAWYERS AG, Zürich

Abkürzung der Firma / Organisation : LLAG
Adresse : Seegartenstrasse 2, Postfach 360, 8024 Zürich
Kontaktperson : RA Dr. Christian Laux
Telefon : 044 880 24 24
E-Mail : christian.laux@lauxlawyers.ch

Datum : 4. April 2017

Wichtige Hinweise:

1. Wir bitten Sie keine Formatierungsänderungen im Formular vorzunehmen und nur die grauen Formularfelder auszufüllen.

2 .Bitte pro Artikel, Absatz und Buchstabe oder pro Kapitel des erläuternden Berichtes eine Zeile verwenden.

3. Ihre elektronische Stellungnahme senden Sie bitte **als Word-Dokument** bis am 4. April 2017 an folgende E-Mail Adresse: jonas.amstutz@bj.admin.ch

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Bundesbeschluss über die Genehmigung und die Umsetzung des Notenaustausches zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz von Personendaten im Bereich der Strafverfolgung und der Rechtshilfe in Strafsachen

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
LAUX LAWYERS AG [LLAG-1]	Wir verweisen hier auf unser Begleitschreiben und die diesem angehängten Separatdokumente. Wir bitten Sie höflich um inhaltliche Auseinandersetzung mit diesen und würden uns freuen, diese im Gespräch bei Bedarf zu verdeutlichen.

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf)

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
LAUX LAWYERS AG [LLAG-2]	DSG	3		e	Antrag: Korrektur der folgenden Definitionen: **Bekanntgabe / Bekanntgeben**: Offenbaren von Personendaten an einen Dritten, der nicht Auftragsdatenbearbeiter ist. Begründung: **Für die vorgenannten, wesentlichen Begriffe, fehlen z.T. Definitionen, was in der Praxis der Digitalisierungsbestrebungen von Unternehmen teilweise zu Problemen führt.** Die Begriffe „Übermittlung", „Übertragung" und „Bekanntgabe" sollten konsequent mit unterschiedlichem Gehalt verwendet werden, wobei zusätzlich der Begriff der Offenbarung als wesentliches Abgrenzungskriterium definiert werden sollte (zur Abgrenzung zwischen code layer und content layer siehe Weber/Laux/Oertly, Datenpolitik als Rechtsthema, Zürich 2016, 5), wie folgt: • Übermittlung: Übermittlung liegt vor, wenn einer der folgenden Vorgänge gemeint ist: (i) Verschiebung Daten von einem Datenträger auf einen anderen Datenträger, sei es nun ein eigener Datenträger oder ein Datenträger eines Dritten, ungeachtet des Umstands, ob ein Offenbaren resultiert (auf dem content layer) oder nicht (z.B. wenn nur verschlüsselte Daten übermittelt werden); (ii) Offenbaren von Informationen (Personendaten) an einen Dritten ausserhalb einer Datenspeicherung (blosse Einsichtnahme). Dieser Begriffsgehalt dürfte in Art. 5 und 6 VE-DSG gemeint sein. • Übertragung: Übertragung meint den der Auftragsdatenbearbeitung vorgelagerten Vorgang, wobei nach der bisher geltenden Rechtslage keine Differenzierung vorgenommen wurde danach, ob (a) der Auftragsdatenbearbeiter nur intransparente Daten bearbeitet (d.h. im Normalbetrieb ohne Zugriff auf die Inhaltsebene, wie es z.B. für einen modern organisierten Betreiber von Rechenzentren der Fall ist) oder ob (b) der Auftragsdatenbearbeiter in einer für ihn transparenten Weise auch die Inhaltsebene (content layer) bearbeitet (wie es z.B. für einen Dienstleister der Fall ist, der eine Versicherungsgesellschaft im Underwriting unterstützt). Übertragung ist ein Unterfall der Übermittlung. • Bekanntgabe: Bekanntgabe meint das Zugänglichmachen von Personendaten bei gleichzeitiger Offenbarung (oder Möglichkeit zur Kennntnisnahme) ohne dass ein Fall der Auftragsdatenbearbeitung gemäss Art. 7 VE-DSG (d.h. eine „Übertragung") vorliegt. Der Begriff der Bekanntgabe wird in Art. 5 und 6 sowie in Art. 13 und 14 VE-DSG thematisiert. Bekanntgabe ist ebenfalls ein Unterfall der Übermittlung. • Offenbaren: Einsichtnahme in den content layer von Personendaten, d.h. unter tatsächlicher Möglichkeit des Erkennens des inhaltlichen Gehalts von Personendaten (z.B. Ansicht mithilfe einer Applikation, mithilfe eines Bildschirms, oder dergleichen). Einordnung in Kürze: • Klärung der Begrifflichkeit führt zu Klärung wichtiger Konzepte im DSG
LAUX LAWYERS AG [LLAG-3]	DSG	3		Neu	Antrag: Aufnahme der folgenden Definition: **Übermittlung / Übermitteln**: Zugänglichmachen von Personendaten in Form der Bekanntgabe, der Übertragung. Eine Übermittlung liegt auch vor, wenn Personendaten in Verbindung mit Massnahmen, die eine Offenbarung ausschliessen, einem Dritten zugänglich gemacht werden. Begründung: siehe den Kommentar zu Art. 3 lit. e VE-DSG. Einordnung in Kürze: • Klärung der Begrifflichkeit führt zu Klärung wichtiger Konzepte im DSG
LAUX LAWYERS AG [LLAG-4]	DSG	3		Neu	Antrag: Aufnahme der folgenden Definition: **Übertragung / Übertragen**: Einbezug eines Auftragsbearbeiters in die Bearbeitung von Personendaten, mit oder ohne Offenbarung der Personendaten gegenüber dem Auftragsbearbeiter. Begründung: siehe den Kommentar zu Art. 3 lit. e VE-DSG. Einordnung in Kürze: • Klärung der Begrifflichkeit führt zu Klärung wichtiger Konzepte im DSG
LAUX LAWYERS	DSG	3		Neu	Antrag: Aufnahme der folgenden Definition:

AG [LLAG-5]					**Offenbarung / Offenbaren**: Ermöglichen der Einsichtnahme in die in Personendaten enthaltenen Angaben (content layer). Begründung: siehe den Kommentar zu Art. 3 lit. f VE-DSG. Einordnung in Kürze: • Klärung der Begrifflichkeit führt zu Klärung wichtiger Konzepte im DSG
LAUX LAWYERS AG [LLAG-6]	DSG	3		i	Antrag: Anpassung von Art. 3 lit. i wie folgt: *Auftragsdatenbearbeiter: Bundesorgan oder private Person, das oder die im Auftrag des Verantwortlichen Personendaten bearbeitet.* Begründung: Anpassung an die Begrifflichkeiten in der europäischen Gesetzgebung. Inhaltlich ist die in der EU gebräuchliche Begriffsverwendung zutreffender. Es geht beim Auftragsdatenbearbeiter nicht darum, dass er *irgendeinen* Auftrag des Verantwortlichen ausführt, sondern es geht darum, dass der Auftrag sich auf die Bearbeitung von Daten (Personendaten) bezieht. Die möglicherweise aus sprachlichen Gründen gewollte Vereinfachung ist ein unnötiges Abweichen vom EU-weiten Verständnis. Einordnung in Kürze: • Swiss Finish (nur Begriffliches)
UX LAWYERS AG [LLAG-7]	DSG	5	2		Antrag: Anpassung von Art. 5 Abs. 2 wie folgt: *Personendaten dürfen ins Ausland bekannt gegeben werden, wenn ~~der Bundesrat festgestellt hat, dass~~ die Gesetzgebung des betreffenden Staates einen angemessenen Schutz gewährleistet. Soweit der Bundesrat die Angemessenheit festgestellt hat, gilt der Nachweis für einen angemessenen Schutz ohne Weiteres als erbracht.* Begründung: Nach Art. 5 Abs. 2 in Verbindung mit Art. 5 Abs. 3 VE-DSG ist die Übermittlung von Personendaten in einen Staat, für den der Bundesrat den angemessenen Schutz (noch) nicht festgestellt hat, grundsätzlich unzulässig. Dies ist zu schablonenhaft und auch zu schwerfällig. Entscheidend ist, ob das Zielland für das konkrete Vorhaben einen angemessenen Schutz bietet (was der Verantwortliche freilich wird nachweisen müssen, wenn kein Bundesratsentscheid vorliegt). Wer einen Cloud Anbieter einsetzt, bleibt in der Verantwortung, aber Beweismittelbeschränkungen zum Nachweis, dass der Schutz angemessen ist, sind fehl am Platz. Der Verantwortliche sollte unter Art. 5 Abs. 3 lit. b jegliche Form von „spezifischen Garantien“ nachweisen können. Die Liste des Bundessrats sollte für aufgeführte Staaten eine Positivliste sein, auf die sich der auslagerungswillige Verantwortliche verlassen dürfen. Einordnung in Kürze: • formaler Compliance-Ansatz statt risikobasierter Regelung
LAUX LAWYERS AG [LLAG-8]	DSG	5	5		Antrag: Reaktionsfrist des Beauftragten ist auf 30 Tage zu reduzieren. Begründung: Die Frist zur Genehmigung ist mit einem halben Jahr zu lange angesetzt. In Bezug auf Binding Corporate Rules (Art. 5 Abs. 3 lit. d) ist nicht einzusehen, inwiefern neu statt wie bisher 30 Tagen (Erledigungsfrist) eine (durch Nachfrage oder Beschwerdeverfahren) sich in die Länge ziehende Frist von 6 Monaten notwendig sein soll. In Bezug auf standardisierte Vertragsgarantien ist die Sechsmonatsfrist noch weniger nachvollziehbar, handelt es sich doch um Vertragsstandards, die der Beauftragte ja schon kennt (hat er sie doch selber ausgestellt, anerkannt oder genehmigt, wie Art. 5 Abs. 3 lit. c VE-DSG klarstellt). Einordnung in Kürze: • Sachfremde Regelung • Widerspricht dem Ziel, die Wettbewerbsfähigkeit der Schweiz zu stärken
LAUX LAWYERS AG [LLAG-9]	DSG	5	6		Antrag: Art. 5 Abs. 6 ist ersatzlos zu streichen. Begründung: Die pauschale Informationspflicht bietet weder der betroffenen Person noch dem EDÖB einen Mehrwert; die EU GDPR kennt eine entsprechende Informationspflicht auch nicht. Einordnung in Kürze: • Swiss Finish
LAUX LAWYERS AG [LLAG-10]	DSG	7	3		Antrag: Präzisierung dahingehend, dass vor Beizug von Subunternehmern nicht jeweils eine Zustimmung im Einzelfall erforderlich ist, sondern eine pauschale Genehmigung des Beizugs – wie in Art. 28 EU-GDPR – genügt. Begründung:

					Eine vorgängige schriftliche Zustimmung ist in der Praxis kaum umsetzbar. Die Regelung sollte analog Art. 28 Abs. 2 DSGVO ausgestaltet werden, wonach die Zustimmung zur Übertragung an einen anderen Auftragsbearbeiter in allgemeiner Form erfolgen kann, mit einem Einspruchsrecht des Verantwortlichen bei Änderungen. Dem VE-DSG ist zu Gute zu halten, dass dies wohl auch so gemeint ist und eine Abweichung zur EU-DSGVO gar nicht beabsichtigt ist. Allerdings ist die Präzisierung notwendig. Einordnung in Kürze: • Sachfremde Regelung • Widerspricht dem Ziel, die Wettbewerbsfähigkeit der Schweiz zu stärken
LAUX LAWYERS AG [LLAG-11]	DSG	12			Antrag: Streichung von Art. 12 VE-DSG. Begründung: Die Regelung ist erbrechtlicher Natur und verallgemeinert Szenarien, die sich letztlich auf die Herausgabe von Daten von Social Media Plattformen beziehen. Sie ist inhaltlich nicht notwendig. Gegebenenfalls sollte die Fragestellung in verallgemeinerter Form im Rahmen der Diskussion zum Recht auf Kopie / Recht auf Datenportabilität geführt werden. Einordnung in Kürze: • Relevanz im Kontext Recht auf Kopie
LAUX LAWYERS AG [LLAG-12]	DSG	13	4		Antrag: Streichung. Begründung: Die Bestimmung ist systemwidrig. Die Auftragsdatenbearbeitung basiert auf dem Konzept einer Privilegierung (der Auftragsdatenbearbeiter ist der „lange Arm“ des Verantwortlichen; alles, was der Verantwortliche darf, darf er auch durch einen Auftragsdatenbearbeiter ausführen lassen). Damit ist nur die Bekanntgabe (Übermittlung von Personendaten an Dritte ohne Bindung) datenschutzrechtlich relevant. Dieses Konzept würde mit einer Informationspflicht bei Einsetzen eines Dritten durchbrochen. Solange der Verantwortliche einen Auftragsdatenbearbeiter rechtmässig und unter Einhaltung der gesetzlich vorgeschriebenen Sicherungsmassnahmen beizieht, besteht kein Anlass für eine Information. Die Bestimmung hat neben anderen nachteiligen Wirkungen insbesondere auch **bremsenden Einfluss auf die Digitalisierung der Schweiz**, namentlich wenn es um den Einsatz von IT-Dienstleistern als Auftragsdatenbearbeiter geht: Die Möglichkeit, IT-Dienstleister – namentlich Cloud-Anbieter – beizuziehen, ist von zentraler Bedeutung (Erhöhung der Agilität und der technischen und organisatorischen Sicherheit bei einem spezialisierten Anbieter). Bereits Art. 7 Abs. 4 VE-DSG zeigt (wie das bisherige Recht), dass jedenfalls der IT-Dienstleister nicht als Dritter zu bezeichnen ist. Die (wie erwähnt) systemwidrige Einführung einer Informationspflicht im Fall einer Bearbeitung von Personendaten über einen Auftragsdatenbearbeiter (z.B. Speicherung von Daten in den Rechenzentren eines spezialisierten Anbieters) würde völlig zu Unrecht suggerieren, dass aus einer Auftragsdatenbearbeitung per se zusätzliche Risiken resultieren und umgekehrt beispielsweise der Betrieb eigener Rechenzentren (nota bene ggf. auch ohne die dazu notwendigen internen Kompetenzen) sicherer ist, als die Auslagerung dieser Aufgabe an einen spezialisierten Anbieter. Dies wäre offensichtlich falsch und somit ist Art. 13 Abs. 4 VE-DSG geradezu gegenläufig zu den Interessen der betroffenen Person (das Gesetz muss den Beizug von spezialisierten IT-Dienstleistern begünstigen, nicht erschweren). Einordnung in Kürze: • Systemwidrige Regelung
LAUX LAWYERS AG [LLAG-13]	DSG	16			Antrag: Im Sinne eines Minimalantrags (aus der Optik Cloud Computing) sollte Art. 16 Abs. 1 VE-DSG wie folgt geändert werden: Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so muss der Verantwortliche ~~oder der Auftragsbearbeiter~~ vorgängig eine Datenschutz-Folgenabschätzung durchführen. Begründung: Keine direkte Pflicht des Auftragsdatenbearbeiters: Nur der Verantwortliche ist hier in die Pflicht zu nehmen. Wenn auch der Auftragsdatenbearbeiter in die Pflicht genommen würde, entstünde ein direkter Widerspruch zu Art. 7 Abs. 4 VE-DSG. In eher allgemeiner Weise ist anzumerken, dass die Datenschutzfolgeabschätzung an sich obsolet wäre. Die Forderung von Art. 8bis der Konvention 108, bei geplanten Datenbearbeitung die Risiken einzuschätzen, wird durch Art. 11 des Vorentwurfs (Datensicherheit) bereits erfüllt. Die interne Dokumentationspflicht nach Art. 19 lit. a VE-DSG ist ausreichend. Einordnung in Kürze: • Systemwidrige Regelung
LAUX LAWYERS AG [LLAG-14]	DSG	17	4		Antrag: Art. 17 Abs. 4 ist wie folgt neu zu formulieren: Der Auftragsdatenbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung, die in der vom Auftragsdatenbearbeiter zu kontrollierenden Sphäre eintritt. Begründung:

					Mit Blick auf die Strafsanktion in Art. 50 Abs. 3 lit. b VE-DSG (Busse bis CHF 500'000) sind die Risikosphären zwischen dem Verantwortlichen und dem Auftragsdatenbearbeiter auch im Tatbestand von Art. 17 Abs. 4 VE-DSG abzugrenzen. Wenn auch der Auftragsdatenbearbeiter in die Pflicht genommen würde, entstünde ein direkter Widerspruch zu Art. 7 Abs. 4 VE-DSG. Ganz generell muss in Bezug auf das Institut „Data Breach Notification“ angemerkt werden, dass die Blossstellungssanktion dieses Instruments systematisch zunächst nur in der US-amerikanischen Rechtsordnung sinnvoll ist (in den USA gilt ein stärker „transaktionaler“, d.h. auf Transaktionen fokussierender Datenschutz, während das CH-Recht (und auch das EU-Recht) mit der Begründung von subjektiven Datenschutzansprüchen einen anderen Ansatz verfolgt). Einordnung in Kürze: • Systemwidrige Regelung
LAUX LAWYERS AG [LLAG-15]	DSG	18	1 und 2		Antrag: Art. 18 Abs. 1 ist wie folgt neu zu formulieren: Der Verantwortliche ~~und der Auftragsbearbeiter sind~~ist verpflichtet, angemessene Massnahmen zu treffen, die ab dem Zeitpunkt der Planung der Datenbearbeitung das Risiko von Verletzungen der Persönlichkeit oder der Grundrechte verringern und solchen Verletzungen vorbeugen. Art. 18 Abs. 2 ist wie folgt neu zu formulieren: Er ist~~Sie sind~~ darüber hinaus verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind. Begründung: Mit Blick auf die Strafsanktion in Art. 51 Abs. 1 lit. e VE-DSG (Busse bis CHF 500'000) sind die Risikosphären zwischen dem Verantwortlichen und dem Auftragsdatenbearbeiter auch im Tatbestand von Art. 18 Abs. 1 VE-DSG abzugrenzen. Wenn auch der Auftragsdatenbearbeiter in die Pflicht genommen würde, entstünde ein direkter Widerspruch zu Art. 7 Abs. 4 VE-DSG. Der Verantwortliche hat – wie bereits Art. 7 Abs. 2 VE-DSG als Voraussetzung für eine Übertragung im Sinne von Art. 7 VE-DSG verlangt – dafür zu sorgen, dass der Auftragsdatenbearbeiter die von ihm benötigten Massnahmen zur Verfügung stellt, damit er als Verantwortlicher seinen Pflichten nach Art. 18 VE-DSG nachkommen kann. Dies hat der Auftragsdatenbearbeiter allerdings nur auf Instruktion bereitzustellen (selbstverständlich werden Cloud-Anbieter aus eigenem Antrieb solche Massnahmen bereitstellen). Inwiefern diese aber für die Zwecke des Verantwortlichen tauglich sind – und dies ist die allein relevante Frage, weil der Auftragsdatenbearbeiter die ihm zugänglich gemachten Daten ja gerade nicht zu eigenen Zwecken bearbeiten darf, wenn er die Stellung als (im Sinne von Art. 7 Abs. 4 VE-DSG privilegierter) Auftragsdatenbearbeiter nicht verlieren soll –, muss nicht der Auftragsdatenbearbeiter entscheiden; dies liegt in der Verantwortung des Cloud-Kunden, der seine Rolle als Verantwortlicher wahrzunehmen hat. Einordnung in Kürze: • Systemwidrige Regelung
LAUX LAWYERS AG [LLAG-16]	DSG	19		b	Antrag: Art. 19 lit. b ist zu streichen, mitsamt der entsprechenden Strafbestimmung. Begründung: Nicht umsetzbar, führt zu Informationsflut. In gewissen Fällen ist die vorgesehene Informationspflicht schlichtweg sinnlos, z.B., wenn Personendaten gelöscht werden, weil sie nicht mehr benötigt werden. Einordnung in Kürze: • Praktikabilität / Sinnhaftigkeit der Regelung • Schädliche Überinformation / mehr Information resultiert nicht in mehr Datenschutz • Systemwidrig, soweit der Auftragsdatenbearbeiter verpflichtet sein soll
LAUX LAWYERS AG [LLAG-17]	DSG	20	5		Antrag: Art. 20 Abs. 5 VE-DSG ist wie folgt zu ändern: Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig. Der Auftragsbearbeiter ist hingegen auskunftspflichtig, wenn er die ihm vorliegenden Angaben zum Verantwortlichen nicht bekannt gibt~~, wer der Verantwortliche ist, oder wenn dieser keinen Wohnsitz in der Schweiz hat.~~ Begründung: Die Regelung in Art. 20 Abs. 5 Satz 2 VE-DSG ist wenig vorteilhaft für Cloud-Anbieter mit Sitz in der Schweiz. Die Regelung würde von Cloud-Anbietern mit Sitz in der Schweiz verlangen, dass sie ähnlich einer Bank ein Know Your Customer-Dossier anlegen (um den Kunden konkret identifizieren zu können). Sollten sie dies nicht tun, müssten sie Auskunft geben zu Nutzungshandlungen, zu denen sie gar nichts aussagen können (weil sie eben gemäss technischem Setup keinen Zugriff auf die Datenbearbeitungsvorgänge auf ihren IT-Infrastrukturen nehmen bzw. nicht nehmen wollen). Ad absurdum geführt: Die Regelung würde einem Cloud-Anbieter geradezu vorgeben, eben doch auf Daten des Cloud-Kunden Zugriff zu nehmen, um für den Ernstfall (Auskunftspflicht) gewappnet zu sein. Das kann nicht gewollt sein. (Pro Memoria: Gemäss Art. 50 Abs. 1 lit. a VE-DSG soll eine Verletzung der Auskunftspflicht mit Busse bis zu CHF 500'000 bestraft werden können). Mit der Regelung, dass diese Situation stets dann eintreten soll, wenn der Cloud-Kunde im Ausland seinen Sitz oder Wohnsitz hat, werden Cloud-Anbieter mit Sitz in der Schweiz und weltweitem Kundenkreis systematisch eingeschränkt. Diese Regelung verstösst klar gegen den Wunsch des Bundesrats, die Wettbewerbsfähigkeit der Schweiz zu stärken.

					Einordnung in Kürze: • Systemwidrige Regelung • Schwächung des Wirtschaftsstandorts Schweiz
LAUX LAWYERS AG [LLAG-18]	DSG	44	3		Antrag: Art. 44 Abs. 3 VE-DSG ist zu löschen. Begründung: Vorsorgliche Massnahmen im Bereich von Datenbearbeitungen können zerstörerische Konsequenzen für Unternehmen haben. Sie können einen Betrieb lahmlegen. Es sollte dem Gericht aufgrund des konkreten Einzelfalles überlassen sein zu entscheiden, die aufschiebende Wirkung zu entziehen. Da von dieser Wirkung auch geplante Cloud-Auslagerungsvorhaben betroffen sein könnten, ist diese Bestimmung auch im vorliegenden Kontext zu nennen. Einordnung in Kürze: • Unbegründeter Eingriff in das Prozessrecht
LAUX LAWYERS AG [LLAG-19]	DSG	50 ff.			Antrag: Das Sanktionenkonzept ist gesamthaft zu überdenken. Strafsanktionen gegen Individuen sind nicht vorzusehen, es sei denn, es solle ganz direkt kriminelle Energie eines Einzelnen ausserhalb seiner organisatorischen Stellung im Unternehmen z.B. des Verantwortlichen sanktioniert werden.
LAUX LAWYERS AG [LLAG-20]	DSG	59			Antrag: Art. 59 ist gesamthaft zu überdenken. Im Sinne von Bestandes- und Vertrauensschutz sind getätigte Investitionen namentlich von Cloud-Kunden zu schützen. Begründung: Bereits bestehende technische Cloud-Setups sollte ein Kunde nicht allein deswegen aufgeben müssen, weil revidierte Datenschutzgesetz in Kraft tritt. Es besteht Bedarf für angemessene Übergangsbestimmungen.