Your World First

C/M/S/
Law.Tax

Newsletter
April 2017

Das neue Datenschutzrecht – die wichtigsten Regelungen im direkten Vergleich

EU-Datenschutz-Grundverordnung (EU-DSGVO), Schweizer Datenschutzgesetz (DSG) und Vorentwurf zum neuen Schweizer DSG

Das neue Datenschutzrecht: neue Herausforderungen für Unternehmen

Nach Jahren ohne wesentliche Änderungen steht das Datenschutzrecht im Zuge der technologischen und gesellschaftlichen Veränderungen nun vor einer radikalen Transformation – in der EU und in der Schweiz.

Die neue EU-Datenschutz-Grundverordnung

Anders als die bisherige EU-Datenschutzrichtlinie 95/46/EG gilt die neue EU-Datenschutz-Grundverordnung unmittelbar in allen 28 EU-Ländern. Sie wird ab dem 25. Mai 2018 anwendbar sein. Das neue Recht erhöht die Transparenz von Datenbearbeitungen und erweitert die Rechte der betroffenen Personen. Verstösse werden mit erheblichen Strafen sanktioniert.

Bedeutung für die Schweiz

Die EU-Datenschutz-Grundverordnung betrifft nicht nur in der EU niedergelassene Unternehmen, sondern unmittelbar auch ausländische Unternehmen, die ihr Angebot an einen bestimmten nationalen Markt in der EU richten oder deren Datenverarbeitung der Beobachtung des Verhaltens von Personen in der EU dient.

Die Schweiz wird sich zudem an die EU-Datenschutz-Grundverordnung anpassen, u. a. mit dem Ziel, wieder einen positiven Angemessenheitsbeschluss der Europäischen Kommission zu erhalten und damit als Land mit „angemessenem Datenschutzniveau" grenzüberschreitenden Datenverkehr mit der EU zu ermöglichen.

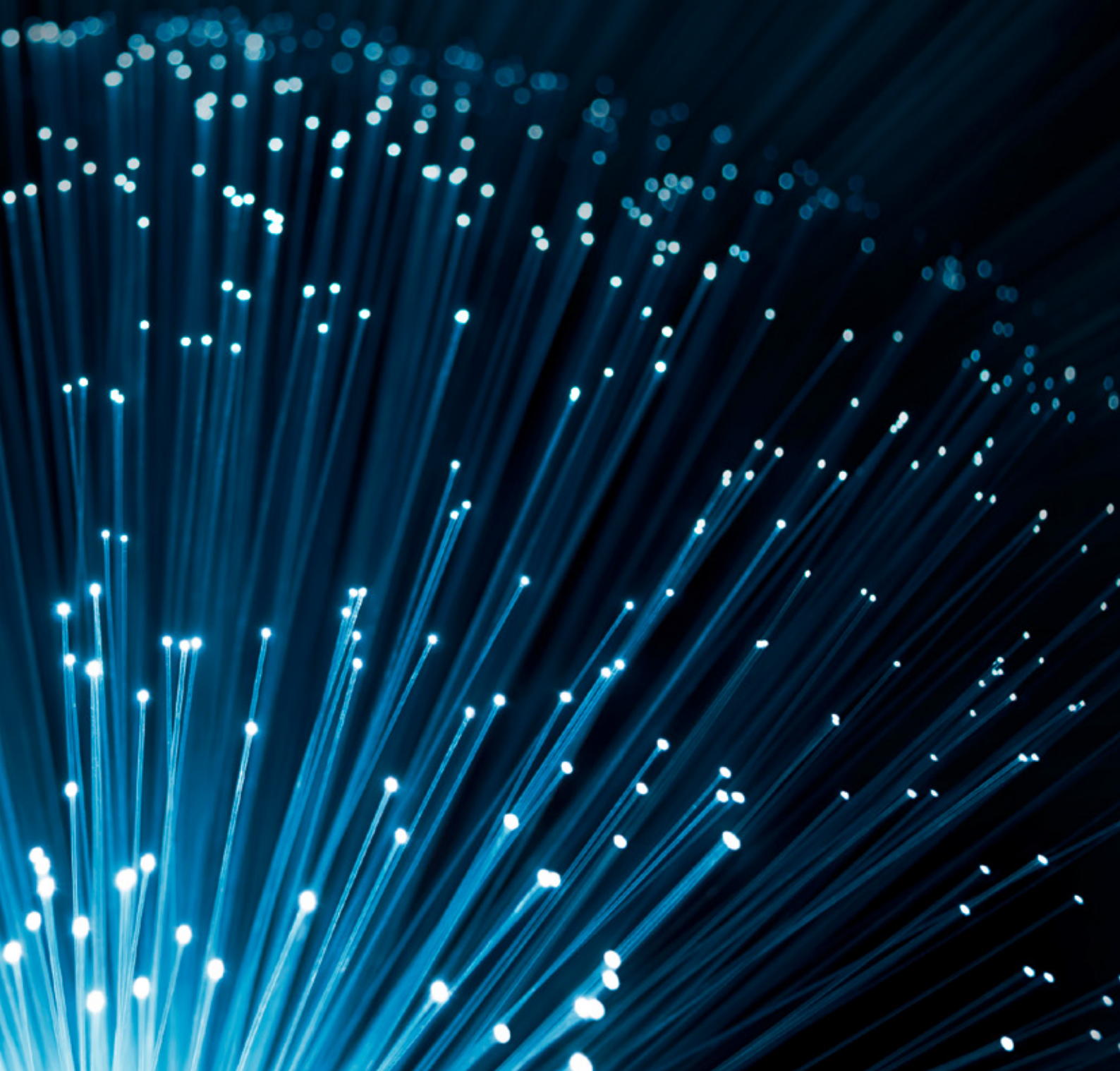
Revision des Datenschutzrechts in der Schweiz

Angesichts des neuen Datenschutzrechts in der EU ist auch das Schweizer Datenschutzgesetz in Revision. Der Bundesrat hat den Vorentwurf zu einer Totalrevision des Datenschutzgesetzes am 21. Dezember 2016 in die Vernehmlassung geschickt.

Dieser Newsletter vermittelt einen ersten Überblick über die wesentlichen Neuerungen des neuen Datenschutzrechts – mit direktem Vergleich zwischen der neuen EU-Datenschutz-Grundverordnung, dem bisher geltenden Schweizer Datenschutzgesetz und dem Vorentwurf zum neuen Schweizer Datenschutzgesetz.

CMS Schweiz
Caroline Gaul, LL.M.
Rechtsanwältin
(Rechtsanwaltskammer Frankfurt am Main)
T +41 44 285 11 11
E caroline.gaul@cms-vep.com

EU-Datenschutz-Grundverordnung (EU-DSGVO), Schweizer Datenschutzgesetz (DSG) und Vorentwurf zum neuen Schweizer DSG



EU-DSGVO

Hintergrund:
Die neue EU-Datenschutz-Grundverordnung löst die EU-Datenschutzrichtlinie 95/46/EG ab und gilt aufgrund ihrer Natur als Verordnung – anders als die alte Richtlinie – unmittelbar in allen 28 EU-Ländern. Sie enthält aber eine Vielzahl von Öffnungsklauseln, die dem nationalen Gesetzgeber wiederum einen gewissen Spielraum geben (z. B. für den Beschäftigtendatenschutz, Verpflichtung zur Bestellung eines Datenschutzbeauftragten). Sie ist ab 25. Mai 2018 anwendbar.

Räumlicher Geltungsbereich

Marktortprinzip:
Die EU-DSGVO gilt nicht nur für die in der EU niedergelassenen Unternehmen, sondern auch für ausländische Unternehmen, die ihr Angebot an einen bestimmten nationalen Markt in der EU richten oder deren Datenverarbeitung der Beobachtung des Verhaltens von Personen in der EU dient.

Indizien für EU-Bezug: Sprache einer Website alleine reicht nicht, aber die Kombination aus Sprache/Währung und der Möglichkeit der Bestellung in dieser Sprache oder der Nennung von Referenzkunden in der EU.

Im Falle des Marktortprinzips: Pflicht zur schriftlichen Bestellung eines Vertreters in der EU. Ausnahmen bestehen (nur gelegentliche Bearbeitung nicht sensibler Daten ohne Risiko). Die Benennung eines Vertreters berührt die Verantwortung oder Haftung des Verantwortlichen oder Auftragsverarbeiters nicht.

Schweiz (bisheriges Gesetz)

Hintergrund:
Das bisherige DSG ist seit 1993 in Kraft. Derzeit profitiert die Schweiz von einem Angemessenheitsbeschluss der Europäischen Kommission, d. h. die Schweiz wird als Land mit angemessenem Datenschutz angesehen, was grenzüberschreitenden Datenverkehr mit der EU ermöglicht.

Räumlicher Geltungsbereich

Öffentlich-rechtliche Vorschriften:
Territorialitätsprinzip;

Privatrechtliche Vorschriften:
gemäss Art. 139 IPRG:
nach Wahl der betroffenen Person:
(1) Ort des Geschädigten oder
(2) Ort des Verletzungserfolgs oder
(3) Ort des Verletzers.

Schweiz (Vorentwurf zum neuen DSG)

Hintergrund:
Der Vorentwurf passt sich stark an die EU-DSGVO an, u. a. mit dem Ziel, die revidierte Europarats-Konvention (Datenschutzkonvention SEV 108) zu ratifizieren und wieder einen positiven Angemessenheitsbeschluss der Europäischen Kommission zu erhalten. Die EU-Kommission wird die „Angemessenheit" 2018 erneut überprüfen.

Räumlicher Geltungsbereich

Öffentlich-rechtliche Vorschriften:
Territorialitätsprinzip;

Privatrechtliche Vorschriften:
gemäss Art. 139 IPRG:
nach Wahl der betroffenen Person:
(1) Ort des Geschädigten oder
(2) Ort des Verletzungserfolgs oder
(3) Ort des Verletzers.

EU-DSGVO

Persönlicher Geltungsbereich:
Daten juristischer Personen sind nicht geschützt.

Informationspflicht / Wichtig für Datenschutzerklärungen:
Proaktive, noch umfangreichere, detailliert geregelte Informationspflicht zum Zeitpunkt der Erhebung der Daten, u. a. Dauer der Speicherung, Rechte der betroffenen Person, Rechtsgrundlage, Bestehen einer automatisierten Entscheidungsfindung.

Form: Kein Formerfordernis, aber die Information muss in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache (ggfs. Verwendung zusätzlicher visueller Elemente) erfolgen.

Recht auf Auskunft:
Sehr detaillierte Auskunftspflicht auf Verlangen. Kostenlos, aber für weitere Kopien kann der Verantwortliche ein angemessenes Entgelt verlangen.

Schweiz (bisheriges Gesetz)

Persönlicher Geltungsbereich:
Daten juristischer Personen sind geschützt.

Informationspflicht / Wichtig für Datenschutzerklärungen:
Keine vergleichbare proaktive Informationspflicht.

Nur eine recht überschaubare Pflicht zur Information zum Zeitpunkt der Beschaffung über den Inhaber der Datensammlung, den Zweck und den Empfänger aber nur (!) im Falle der Erhebung besonders schützenswerter Personendaten / Persönlichkeitsprofile.

Recht auf Auskunft:
Auskunftspflicht (welche Daten einschließlich der verfügbaren Angaben über die Herkunft der Daten, Zweck, ggfs. die Rechtsgrundlagen des Bearbeitens sowie die Kategorien der bearbeiteten Personedaten, die an der Sammlung Beteiligten und Datenempfänger). Grundsätzlich kostenlos, aber mit Ausnahmen.

Schweiz (Vorentwurf zum neuen DSG)

Persönlicher Geltungsbereich:
Daten juristischer Personen sind nicht (mehr) geschützt.

Informationspflicht/ Wichtig für Datenschutzerklärungen:
Proaktive Informationspflicht bei allen, nicht mehr nur bei besonders schützenswerten Personendaten oder Persönlichkeitsprofilen.

Umfang: geringer als bei der EU-DSGVO: alle Informationen, die erforderlich sind, damit die betroffene Person ihre Rechte nach diesem Gesetz geltend machen kann, insbesondere Verantwortlicher, bearbeitete Personendaten, Zweck, Empfänger, Auftragsdatenbearbeiter, Bestehen einer automatisierten Einzelentscheidung.

Form: Kein Formerfordernis, aber die Information muss leicht zugänglich, vollständig, genügend sichtbar und verständlich sein. Symbole und Piktogramme können verwendet werden, wenn sie die nötigen Informationen enthalten.

Recht auf Auskunft:
Umfangreichere Auskunftspflicht (Aufbewahrungsdauer, Vorliegen einer automatisierten Einzelentscheidung).

EU-DSGVO

Recht auf Datenübertragung:
Recht auf Datenportabilität (gibt der betroffenen Person die Möglichkeit, ihre Daten zu erhalten und ggfs. an einen anderen Anbieter zu übertragen).

Weitere Rechte der Betroffenen:
Recht auf Berichtigung von Daten.

Recht auf Löschung/Vernichtung von Daten.

Recht auf Einschränkung der Bearbeitung.

Daten Verstorbener:
Die EU-DSGVO gilt nicht für die personenbezogenen Daten Verstorbener und enthält keine Regelungen dazu.

Bekanntgabe ins Ausland:
Daten dürfen grundsätzlich nur ins Ausland bekannt gegeben werden, wenn dort „angemessener Schutz" gemäss Angemessenheitsbeschluss der EU-Kommission besteht.

Ausnahmen bestehen, insbesondere im Fall von EU-Model Clauses, die von der Kommission oder der Aufsichtsbehörde in einem bestimmten Verfahren angenommen werden und Binding Corporate Rules, letztere müssen von der zuständigen Aufsichtsbehörde genehmigt werden, ihr Inhalt ist in der EU-DSGVO geregelt.

Schweiz (bisheriges Gesetz)

Recht auf Datenübertragung:
Keine Datenportabilität.

Weitere Rechte der Betroffenen:
Recht auf Berichtigung von Daten.

Recht auf Löschung nicht ausdrücklich geregelt, folgt aber aus dem Persönlichkeitsrecht.

Recht auf Einschränkung der Bearbeitung nicht ausdrücklich geregelt, folgt aber aus dem Persönlichkeitsrecht.

Daten Verstorbener:
Keine Regelung zu den Daten Verstorbener im DSG (nur Einsichtsrecht in Daten Verstorbener in Bezug auf Daten der betroffenen Person, geregelt im VDSG).

Bekanntgabe ins Ausland:
Daten dürfen grundsätzlich nur ins Ausland bekannt gegeben werden, wenn dort „angemessener Schutz" besteht (siehe nicht verbindliche Liste der Staaten veröffentlicht vom EDÖB).

Ausnahmen bestehen, insbesondere im Fall von EU-Model Clauses und Binding Corporate Rules, die dem EDÖB mitgeteilt werden müssen. Im Fall der Abänderung von Standardverträgen und im Fall von Binding Corporate Rules kann der EDÖB diese innerhalb von 30 Tagen prüfen.

Schweiz (Vorentwurf zum neuen DSG)

Recht auf Datenübertragung:
Keine Datenportabilität.

Grund: Nach Auffassung des Bundesrates ist dieses Recht mehr darauf ausgerichtet, den betroffenen Personen die Wiederverwendung ihrer Daten zu ermöglichen, um den Wettbewerb spielen zu lassen, als ihre Persönlichkeit zu schützen.

Weitere Rechte der Betroffenen:
Recht auf Berichtigung von Daten.

Recht auf Löschung/Vernichtung von Daten ausdrücklich geregelt.

Recht auf Einschränkung der Bearbeitung ausdrücklich geregelt.

Daten Verstorbener:
Regelungen zu den Daten Verstorbener („digitaler Tod").

Bekanntgabe ins Ausland:
Daten dürfen grundsätzlich nur ins Ausland bekannt gegeben werden, wenn dort „angemessener Schutz" besteht. Die Festlegung, welche Staaten das sind, erfolgt neu durch Entscheid des Bundesrates.

Ausnahmen bestehen, insbesondere im Fall von EU-Model Clauses, die vom EDÖB ausgestellt oder anerkannt sind oder von ihm vorgängig genehmigt wurden, oder im Fall von Binding Corporate Rules, die demnächst auch durch eine ausländische Behörde, die für den Datenschutz zuständig ist, vorgängig genehmigt werden können.

EU-DSGVO

Bedeutung des Europäischen Ausschusses:
Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren durch den Europäischen Ausschuss (bestehend aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedsstaats und dem Europäischen Datenschutzbeauftragten).

Automatisierte Einzelfallentscheidung:
Verbot der automatisierten Einzelfallentscheidung.

Beispiel: automatische Ablehnung eines Online-Kreditantrags.

Mit Ausnahmen:
(1) erforderlich für den Vertrag
(2) aufgrund von Rechtsvorschriften der Mitgliedstaaten zulässig oder
(3) ausdrückliche Einwilligung der betroffenen Person.

Datenschutz-Folgenabschätzung:
Birgt die Art der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten, muss der Verantwortliche bereits vorab eine Abschätzung der Folgen für den Schutz personenbezogener Daten durchführen. Dies ist immer der Fall beim Profiling, der Verarbeitung besonders sensibler Daten, und einer umfangreichen Videoüberwachung.

Zeigt die Datenschutz-Folgenabschätzung ein verbleibendes hohes Risiko, muss die Datenschutzaufsichtsbehörde konsultiert werden.

Schweiz (bisheriges Gesetz)

Bedeutung des EDÖB:
Empfehlungen des EDÖB.

Automatisierte Einzelfallentscheidung:
Kein Verbot der automatisierten Einzelentscheidung.

Keine Datenschutz-Folgenabschätzung

Schweiz (Vorentwurf zum neuen DSG)

Bedeutung des EDÖB:
„Empfehlungen der guten Praxis" durch den EDÖB, bei deren Befolgung das DSG eingehalten wird.

Automatisierte Einzelfallentscheidung:
Kein Verbot der automatisierten Einzelentscheidung, aber Informationspflicht.

Zudem: Recht der betroffenen Person, in diesem Fall ihren Standpunkt geltend zu machen.

Ausnahme: Ein Gesetz sieht eine automatisierte Einzelentscheidung vor.

Datenschutz-Folgenabschätzung:
Pflicht zur Datenschutz-Folgenabschätzung und Mitteilungspflicht an den EDÖB.

Der EDÖB hat bereits eine „App" dazu entwickelt:
https://www.apps.edoeb.admin.ch/dsfa/de/index.html

EU-DSGVO

Meldepflicht für Verletzungen:
Verletzungen des Schutzes personenbezogener Daten müssen unverzüglich, möglichst innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls, an die zuständige Aufsichtsbehörde gemeldet werden. Eine Ausnahme besteht, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen führt. Besteht die Wahrscheinlichkeit, dass die Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten bewirkt, muss der Verantwortliche auch die betroffene Person ohne unangemessene Verzögerung benachrichtigen – es sei denn, er hat technisch-organisatorische Massnahmen getroffen, die eine Kenntnisnahme durch Dritte verhindern oder die sicherstellen, dass aller Wahrscheinlichkeit nach kein hohes Risiko mehr für die Rechte und Freiheiten der betroffenen Person besteht.

Privacy by Design und Privacy by Default:
Gesetzliche Verankerung der Grundsätze der Datenvermeidung und Datensparsamkeit durch konkrete gesetzliche Anforderungen:

Privacy bei Design = Datenschutz durch Technik, z. B. Pseudonymisierung

Privacy by Default = Datenschutz durch datenschutzfreundliche Voreinstellung, insbesondere Erhebung nur solcher Daten, die unbedingt erforderlich sind und Speicherung nur so lange wie unbedingt erforderlich.

Schweiz (bisheriges Gesetz)

Keine Meldepflicht

Privacy by Design und Privacy by Default:
Kein ausdrückliches Gesetz, aber „Grundsatz der Verhältnismässigkeit".

Schweiz (Vorentwurf zum neuen DSG)

Meldepflicht:
Der Verantwortliche muss dem EDÖB unverzüglich eine unbefugte Datenbearbeitung oder den Verlust von Daten melden, es sei denn, die Verletzung des Datenschutzes führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person. Der Verantwortliche muss ausserdem die betroffene Person informieren, wenn es zum Schutz der betroffenen Person erforderlich ist oder der EDÖB es verlangt. Dafür wird das Register der Datensammlungen abgeschafft.

Privacy by Design und Privacy by Default:
Privacy by Design und Privacy by Default gesetzlich verankert.

EU-DSGVO

Verzeichnis aller Verarbeitungstätigkeiten:
Pflicht zur Führung eines Verzeichnisses aller Verarbeitungstätigkeiten für den Verantwortlichen und ggfs. seinen Vertreter und den Auftragsdatenbearbeiter. Die erforderlichen Angaben sind in der Verordnung genau bestimmt.

Datenschutzbeauftragter:
Pflicht zur Bestellung eines Datenschutzbeauftragten in bestimmten Fällen (insbesondere bei regelmässiger und systematischer Überwachung von Personen oder Bearbeitung besonders schützenswerter Personendaten).

Aufsichtsbehörde mit umfangreichen Befugnissen:
Verwarnungen, Anweisungen, Verbote, einstweilige Massnahmen, gerichtliche Verfahren anstossen/betreiben oder sich daran beteiligen.

Strafen:
Bussgelder bis zu 4% des Jahresumsatzes eines Unternehmens, beziehungsweise 20 Mio. Euro, wobei der jeweils höhere Wert gilt. Dabei ist auf den gesamten weltweiten Jahresumsatz des betreffenden Unternehmens abzustellen und nicht etwa nur auf den in Europa erwirtschafteten.

Schweiz (bisheriges Gesetz)

Kein Verzeichnis:
Keine Verpflichtung zur Führung eines Verzeichnisses aller Verarbeitungstätigkeiten, allerdings in bestimmten Fällen Pflicht zur Anmeldung von Datensammlungen an den EDÖB und dann auch Pflicht zur Erstellung eines Bearbeitungsreglements sowie Pflicht zur Protokollierung automatisierter Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen, wenn die präventiven Massnahmen den Datenschutz nicht gewährleisten können.

Datenschutzbeauftragter:
Keine Pflicht zur Bestellung eines Datenschutzbeauftragten.

EDÖB kann:
- Empfehlungen aussprechen.
- Popularklage beim BVGer erheben.
- Vorsorgliche Massnahmen beim BVGer beantragen.

Strafen:
Strafbarkeit in wenigen Fällen mit Busse in Höhe von max. 10.000 Franken und nur auf Antrag.

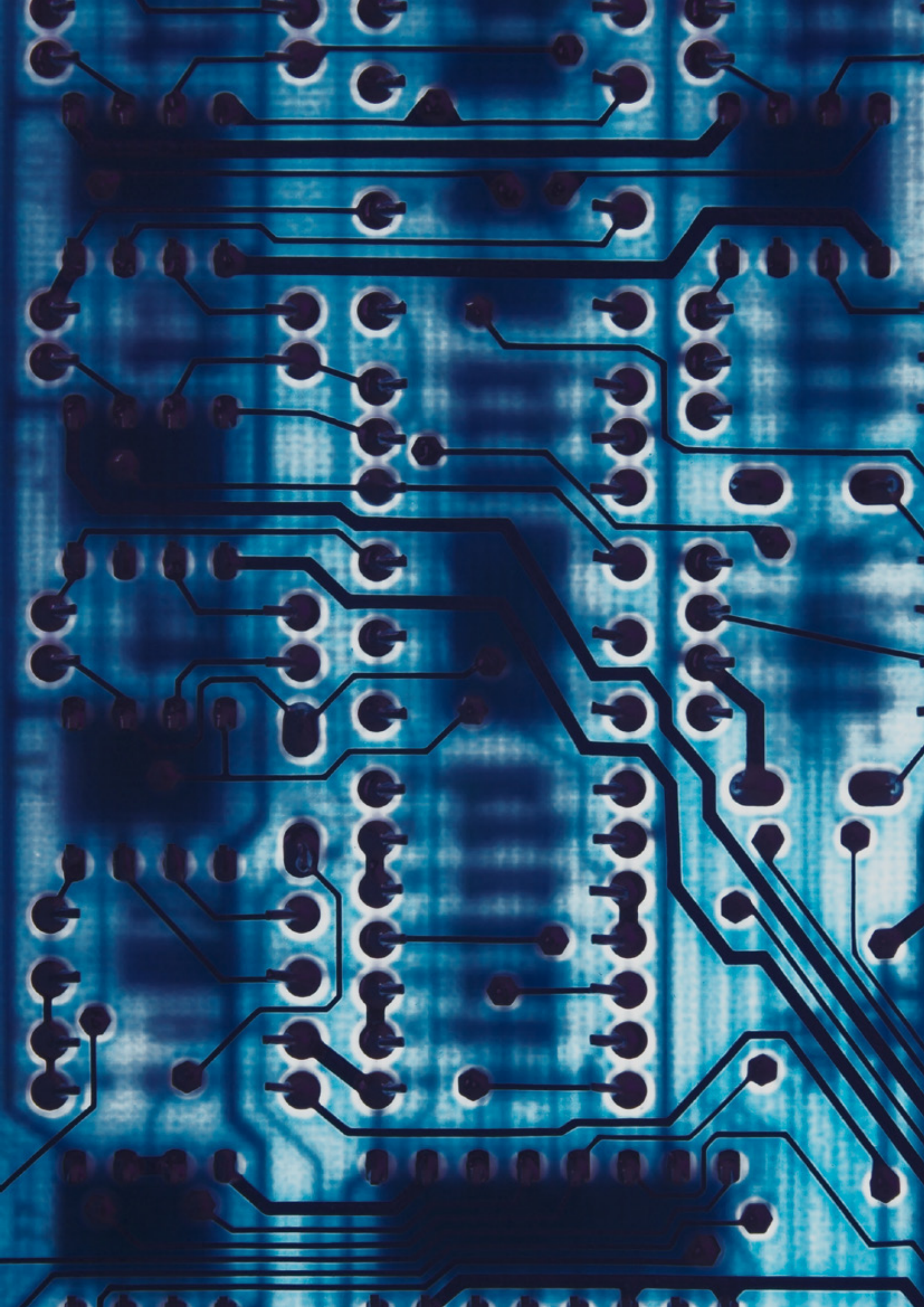
Schweiz (Vorentwurf zum neuen DSG)

Dokumentationspflicht:
Pflicht zur Dokumentation jeder Datenbearbeitung für den Verantwortlichen und den Auftragsdatenbearbeiter. Das Gesetz sieht nicht vor, welche Angaben dokumentiert werden müssen; dies wird in der Verordnung konkretisiert. Die Dokumentation muss jedoch so ausgestaltet sein, dass der Verantwortliche und der Auftragsbearbeiter ihren Informations- und Meldepflichten nachkommen können. Dafür Aufhebung der Pflicht zur Meldung von Datensammlungen an den EDÖB.

Datenschutzbeauftragter:
Keine Pflicht zur Bestellung eines Datenschutzbeauftragten.

EDÖB kann:
- Selbst vorsorgliche Massnahmen verfügen.
- Verwaltungsmassnahmen verfügen (z. B. Bekanntgabe ins Ausland stoppen, Vernichtung der Daten anordnen).

Strafen:
Busse bis zu 500.000 Franken bei Vorsatz und bis zu 250.000 Franken bei Fahrlässigkeit. Gegebenenfalls zu zahlen durch den Geschäftsbetrieb.



C/M/S/ Law-Now™

Law.Tax

Ihr kostenloser juristischer Online-Informationsdienst.

E-Mail-Abodienst für Fachartikel zu vielfältigen juristischen Themen.
cms-lawnow.com

C/M/S/ e-guides

Law.Tax

Ihre juristische Online-Bibliothek.

Profunde internationale Fachrecherche und juristisches Expertenwissen nach Mass.
eguides.cmslegal.com

CMS-Büros und verbundene Büros:
Aberdeen, Algier, Amsterdam, Antwerpen, Barcelona, Belgrad, Berlin, Bogotá, Bratislava, Bristol, Brüssel, Budapest, Bukarest, Casablanca, Dubai, Düsseldorf, Edinburgh, Frankfurt/Main, Genf, Glasgow, Hamburg, Hong Kong, Istanbul, Kiew, Köln, Leipzig, Lima, Lissabon, Ljubljana, London, Luxemburg, Lyon, Madrid, Mailand, Maskat, Medellín, Mexiko-Stadt, Moskau, München, Paris, Peking, Podgorica, Prag, Rio de Janeiro, Rom, Santiago de Chile, Sarajevo, Sevilla, Shanghai, Sofia, Strassburg, Stuttgart, Teheran, Tirana, Utrecht, Warschau, Wien, Zagreb und Zürich.

---

cms.law