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 : swissICT, Schweizerischer Verband der Informations- und Kommunikationstechnologie

Abkürzung der Firma / Organisation : swissICT

Adresse : Vulkanstrasse 120, 8048 Zürich

Kontaktperson : Thomas Flatt

Telefon : +41 43 336 40 24

E-Mail : thomas.flatt@swissict.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!

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

Inhaltsverzeichnis

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) 3

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 Fehler! Textmarke nicht definiert.

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" 29

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

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
swissICT	DSG				**Vorbemerkung:** Die Totalrevision des DSG sollte vor allem • eine Brücke schlagen zwischen Sicherstellung Persönlichkeitsschutz der betroffenen Personen und Schaffung moderner Rahmenbedingungen für einen innovativen Wirtschaftsstandort Schweiz im Zeitalter der Digitalisierung; und • eine unnötige Verschärfung gegenüber den Vorgaben des Europarates und der EU (sog. "Swiss Finish") zu Lasten der Innovation und ohne effektiven Nutzen oder Schutz vermeiden, welche die wirtschaftliche Entwicklung hindert. Mit der Lancierung der Strategie für eine digitale Schweiz präsentiert der Bundesrat eine Dachstrategie (Medienmitteilung des Bundesrates vom 20.4.2016: Strategie des Bundesrates für eine digitale Schweiz), mit welcher die Schweiz mehr von der zunehmenden Digitalisierung profitieren und sich als innovative Volkswirtschaft noch dynamischer entwickelt soll. Die Wirtschaft soll sich im digitalen Raum möglichst frei entfalten können. Gleichzeitig hält der Bundesrat fest, dass für eine informierte und demokratische Gesellschaft und zur Sicherung der Wohlfahrt, die von der Datenbearbeitung betroffenen Personen die modernen Informations- und Kommunikationstechnologien in ihrem täglichen Leben kompetent und sicher nutzen können sollten. Dies bedingt jedoch eine kohärente und zukunftsorientierte Datenpolitik zu entwickeln. Weiter führt der Bundesrat aus, dass sich das Potenzial der vermehrten Sammlung und Bearbeitung von Daten zum Vorteil der Schweiz realisieren muss, ohne die Kontrolle über diese Daten zu verlieren. In diesem Kontext ist daher auch die Revision des Datenschutzgesetzes zu sehen und entsprechend einzuordnen, welche absolut zentral ist für die Weiterentwicklung des Wirtschaftsstandortes Schweiz im Zeitalter der Digitalisierung.

					Aus diesem Grund wird eine Verschärfung gegenüber den Vorgaben des Europarates und der EU (sog. "Swiss Finish") zu Lasten der Innovation und ohne effektiven Nutzen oder Schutz, welche die wirtschaftliche Entwicklung hindert, von swissICT abgelehnt. Die europäische Datenschutz-Grundverordnung (DSGVO) verlangt keine pauschale Übernahme ihrer Bestimmungen. Für die Angemessenheitserklärung genügt es vielmehr, grundlegende Garantien einzuhalten, beispielsweise die Rechtsstaatlichkeit oder die Existenz unabhängiger Aufsichtsbehörden. Die DSGVO hält denn auch ausdrücklich fest, dass die Umsetzung der ERK 108 bei der Angemessenheitsbeurteilung ein wesentlicher Faktor ist. Vor diesem Hintergrund sollte sich das künftige DSG primär an der ERK 108 orientieren. Darüber hinausgehende Regelungen können nur insofern sinnvoll sein, als sie helfen, einen einheitlichen Standard nach Massgabe der DSGVO zu fördern. **Eine Verschärfung des DSG gegenüber der ERK 108 und der DSGVO wäre deshalb konzeptionell falsch, nicht notwendig, zulasten schweizerischer Unternehmen wettbewerbsverzerrend und innovationsfeindlich. Ein sog. „Swiss Finish“ kommt daher nur infrage, wenn er eine Erleichterung mit sich bringt** und zur Attraktivität des Wirtschaftsstandortes der Schweiz und zur Förderung der Innovation und Digitalisierung beiträgt**.**
swissICT	DSG	2	3		**Kernanliegen: Keine Streichung der Regel von Art. 2 Abs. 2 lit. c DSG** Zur Eindämmung des Missbrauchs und um die verfahrensrechtlichen Regeln gemäss den einschlägigen Verfahrensordnungen wie z.B. der ZPO nicht zu verwässern, fordern wir, Art. 2 Abs. 2 lit. c DSG (Nichtanwendbarkeit des DSG auf hängige Zivilprozesse und anderer Verfahren mit Bezug auf sämtliche Verfahren insbesondere auch auf kantonaler Stufe) nicht zu streichen. Es ist ferner nicht einsehbar, weshalb die wichtige und richtige Regel von Art. 2 Abs. 3 VE-DSG nur für bundesrechtliche Verfahren gelten soll. In hängigen Verfahren müssen insbesondere auch kantonale (Vor-) Instanzen gleichermassen rechtlich geschützt sein. Auch der geltende Art. 2 Abs. 2 lit. c DSG bezieht sich auf Verfahren vor allen Instanzen. Vgl. im Einzelnen hinten zu Art. 20 Abs. 1 VE-DSG.

swissICT	DSG	3		f	**Kernanliegen: Streichung des im Vergleich zur DSGVO überschiessenden „Swiss Finish" und Beschränkung auf Personendaten sowie eine automatisierte Bearbeitung.** Die Definition von „Profiling" ist zu breit und geht massiv weiter als die Definition von „Profiling" in der DSGVO: Bereits eine „von Hand" bearbeitete Mitarbeiterbeurteilung würde als "Profiling" nach Art. 23 Abs. 2 Bst. d VE-DSG und damit per se als Persönlichkeitsverletzung gelten. Konsequenterweise müsste ein Bearbeiter vor jeder Bearbeitung einen Rechtfertigungsgrund ausweisen können, falls nicht vorgängig eine ausdrückliche Einwilligung eingeholt worden wäre. Dies stellt für das Profiling einen Paradigmenwechsel im schweizerischen Datenschutzrecht dar, für den es keinen Grund gibt. Zudem umfasst „Profiling" dem Wortlaut des Vorentwurfs nach auch das Bearbeiten von nicht-personenbezogenen Daten, was eine unzulässige Ausweitung des Geltungsbereichs des DSG darstellen und im Widerspruch zu Art. 2 Abs. 1 VE-DSG stehen würde. Schliesslich ist eine Analyse bzw. Auswertung keine Datenbearbeitung, die sich per se negativ auf die Persönlichkeitsrechte der betroffenen Personen auswirkt. Richtigerweise wäre der Begriff „Auswertung" durch „Bewertung" zu ersetzen – erst diese stellt einen datenschutzrechtlich relevanten Eingriff in die Persönlichkeitsrechte der betroffenen Personen dar. „Bewertung" umfasst eine Entscheidung, die sich auf eine Analyse bzw. Auswertung stützt. Die Anknüpfung an die Auswertung greift demnach zu weit.
swissICT	DSG	5			**Kernanliegen: Die Informations- und Genehmigungspflichten setzten komplizierte sowie ressourcenintensive, interne Prozesse voraus. Die Fristen für die Überprüfungen durch den EDÖB sollten auf höchstens vier Wochen reduziert werden.**
swissICT	DSG	5	2 und 3		Art. 5 Abs. 2 und 3 VE-DSG sehen vor, dass der Bundesrat eine Liste von Staaten mit angemessenem Schutz führt. Aus Abs. 3 ergibt sich, dass die Übermittlung in einen Staat, der nicht auf dieser Liste figuriert, grundsätzlich unzulässig ist, vorbehaltlich der Garantien nach art. 5 und der Ausnahmesituationen nach Art. 6 VE-DSG. Die Liste des Bundesrats fingiert also, dass nicht aufgeführte Staaten keinen angemessenen Schutz gewährleisten. Das ist abzulehnen, weil die Anpassung der Liste auf dem Verordnungsweg relevante Rechtsänderungen nicht sofort nachvollziehen kann. Es

					ist zudem denkbar, dass ein Datenbearbeiter über Informationen verfügt, aus denen sich ergibt, dass ein bestimmter Empfängerstaat über ein angemessenes Schutzniveau verfügt, obwohl er nicht auf der Liste des Bundesrats aufgeführt ist. In solchen Fällen führt eine Übermittlung ins Ausland nicht zu einer Gefährdung der betroffenen Personen und damit auch nicht zu einer Verletzung von Art. 5 Abs. 1 VE-DSG. Die Liste des Bundessrats muss daher für aufgeführte Staaten eine Positivliste darstellen, auf die sich Datenbearbeiter verlassen dürfen. Das deckt die Masse der Auslandsübermittlungen ab. Die Liste darf umgekehrt aber keine Negativliste im Sinne einer Fiktion sein. Sie darf höchstens die Vermutung begründen, dass im betreffenden Staat ein angemessener Schutz fehlt. Dem Datenexporteur muss der Beweis des Gegenteils dabei offengelassen werden.
swissICT	DSG	5	3	b	Gemäss lit. b muss der Beauftragte informiert werden, bei lit. d braucht es eine Genehmigung des Beauftragten. Diese unterschiedliche Handhabung ist nicht nachvollziehbar. Worin der Unterschied zwischen Garantien nach lit. b und d besteht, bedarf daher einer Klärung, Der Aufwand für ein Unternehmen sollte verhältnismässig sein und wenn möglich sollte der VE-DSG einheitliche Instrumente/Abläufe vorsehen, was ebenfalls dem EDÖB bei der internen Beurteilung zugute kommt.
swissICT	DSG	5	3	d	Art. 5 Abs. 3 VE-DSG regelt das Vorgehen, wenn der Bundesrat keinen angemessenen Schutz festgestellt hat. In lit. d Ziff. 2 wird als Ausnahme die Genehmigung einer ausländischen Behörde zu einer verbindlichen unternehmensinternen Datenschutzvorschrift erwähnt, sofern diese in einem Staat liegt, welche einen angemessenen Schutz gewährleistet. Unklar ist hierbei, wer beurteilt, dass diese ausländische Behörde einem Staat angehört, die einen angemessenen Schutz gewährleistet.
swissICT	DSG	5	3	d	Die Regelung, wonach die Genehmigung von Binding Corporate Rules (BCR) durch den EDÖB bis zu sechs Monate dauern kann, ist weder sachgerecht noch praktikabel (Art. 5 Abs. 3 lit. d und Abs. 5 VE-DSG). Zudem stellen die BCR eine „Unterkategorie“ der „spezifischen Garantien“ i.S.v. Art. 5 Abs. 3 lit. b VE-DSG dar – und für diese ist lediglich eine Informationspflicht vorgesehen (eine Genehmigung durch den EDÖB ist nicht erforderlich). Dasselbe gilt für die Möglichkeit des EDÖB, Informationen nachzuverlangen (Abs. 5), was die sechsmonatige Frist verlängern würde. Bei einer solchen Regelung würden BCR im Ergebnis nicht mehr verwendet, was dem Regelungsziel von Art. 5 VE-DSG zuwiderläuft.

swissICT	DSG	5	4		Die Frist von 30 Tagen kann bei laufenden Vertragsverhandlungen zu lang sein. Eine kürzere Prüffrist der spezifischen Garantien (Vertrag) von 10 Tagen wäre daher zu begrüssen, um eine Lähmung der Unternehmenstätigkeit zu verhindern.
swissICT	DSG	5	5		Die unterschiedliche Handhabung der spezifischen resp. standardisierten Garantien ist nicht nachvollziehbar. Eine Information gemäss Abs. 3 lit. b sollte ausreichen. Die Frist zur Genehmigung ist mit einem halben Jahr zu lange angesetzt (bisher musste die Prüfung selbst von BCR innert 30 Tagen durchgeführt sein). Hinzu kommt, dass die tatsächliche Frist wiederum sehr viel länger sein kann, da der EDÖB sich jederzeit auf den Standpunkt stellen kann, er habe noch nicht alle erforderlichen Informationen. Erschwerend tritt hinzu, dass bei einem negativen Entscheid ein Unternehmen aufgrund der neuen Verfügungsmacht des EDÖB den Entscheid vor dem Bundesverwaltungsgericht anfechten muss, was zu einer weiteren Verzögerung, bei gleichzeitiger Lähmung der Unternehmenstätigkeit, führt.
swissICT	DSG	5	6		Art. 5 Abs. 6 ist ersatzlos zu streichen. Die pauschale Informationspflicht bietet weder der betroffenen Person noch dem EDÖB einen Mehrwert; die DSGVO kennt eine entsprechende Informationspflicht auch nicht (Art. 5 Abs. 6).
swissICT	DSG	5	7		Abs. 7 dahingehend zu ergänzen, dass der Bundesrat diese Liste aktuell halten muss, da diese neu verbindlichen Charakter für die Unternehmen hat und sich diese darauf verlassen müssen.
swissICT	DSG	6			**Kernanliegen: Berücksichtigung der Bedürfnisse der Praxis bei der Festlegung der Ausnahmetatbestände.**
swissICT	DSG	6	1	a	Im Text des Vorentwurfs ist wie im heutigen Text von einer Einwilligung „im Einzelfall“ die Rede. Diese Begrenzung findet sich nicht in Art. 49 Abs. 1 lit. a DSGVO. Es wäre wichtig, im Text des VE-

					DSG – oder zumindest im Erläuternden Bericht – festzuhalten, dass der „Einzelfall" jeweils die Gesamtheit ähnlich gelagerter Bekanntgaben ins Ausland umfasst. Die Einwilligung muss daher jeweils für alle vergleichbaren Bekanntgaben gelten, wie dies in der heutigen Lehre anerkannt ist.
swissICT	DSG	6	1	b	Art. 6 Abs. 1 lit. b VE-DSG sollte mit der Regelung der DSGVO in Übereinstimmung gebracht werden. Danach sollte eine Bekanntgabe im Sinne eines Ausnahmefalls auch dann zulässig sein, wenn die betroffene Person nicht Vertragspartei ist, aber der fragliche Vertrag in ihrem Interesse oder zu ihren Gunsten abgeschlossen wurde. Art. 6 Abs. 1 lit. b ist daher wie folgt anzupassen: *die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten der Vertragspartnerin oder des Vertragspartners handelt <u>oder einer Person, zu deren Gunsten oder in deren Interesse der Vertrag abgeschlossen wird</u>;*
swissICT	DSG	6	1	c	Um schwierige Abgrenzungsfragen im Voraus auszuschliessen, sollten in Art. 6 Abs. 1 lit. c Ziff. 2 VE-DSG die Begriffe „Gericht" sowie „Verwaltungsbehörde" ersatzlos gestrichen werden. Massgebend ist, dass die Datenbearbeitung zur „Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen" erfolgt. Die hierfür zuständigen ausländischen Behörden können aus historischen Gründen unterschiedlich organisiert sein sowie verschiedene Bezeichnungen tragen und sich nicht in eine der beiden Kategorien zuordnen lassen. Art. 6 Abs. 1 lit. c Ziff. 2 ist daher wie folgt anzupassen: *die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen ~~vor einem Gericht oder einer Verwaltungsbehörde~~;*
swissICT	DSG	6	2		Art. 6 Abs. 2 VE-DSG sollte ersatzlos gestrichen werden. Erstens ist eine Pflicht, den EDÖB trotz Ausnahmetatbestand zu informieren, unverhältnismässig. Zweitens wird diese breite (für Verantwortliche <u>und</u> Auftragsdatenbearbeiter) geltende Pflicht zu einer „*Meldeflut*" führen, welche der EDÖB gar nicht wird bewältigen können. Ferner würde der EDÖB dadurch über heikle Verfahren und (Geschäfts-)Geheimnisse informiert, ohne sachlichen Grund und ohne Mehrwert für betroffene

					Personen. Das greift massiv in die unternehmerische Freiheit und in die durch das ZGB und andere Erlasse weiterhin geschützte Geheimsphäre der Unternehmen ein. Zudem ist diese Pflicht der DSGVO und der Konvention 108 fremd und stellt damit einen abzulehnenden Swiss Finish dar.
swissICT	DSG	7	3		**Auftragsdatenbearbeitung / Sub-Processing** Gemäss Art. 7 Abs. 3 VE-DSG soll eine Weiterübertragung der Auftragsbearbeitung ("Sub-Processing") künftig nur noch mit vorgängiger schriftlicher Zustimmung des Verantwortlichen möglich sein. Im erläuternden Bericht wird darauf verwiesen, die DSGVO sehe "etwa Ähnliches" vor. Dem kann nicht gefolgt werden; die DSGVO enthält keine vergleichbare Bestimmung, womit der VE-DSG hier weiter geht als notwendig. Die strengen Zulässigkeitsvoraussetzungen sind auch in der Sache nicht begründet. Bei der Übertragung der Auftragsbearbeitung an einen Sub-Processor in einem Staat ohne angemessenes Datenschutzniveau finden die Bestimmungen zur Datenbekanntgabe ins Ausland gemäss Art. 5/6 VE-DSG Anwendung und sorgen bereits für hinreichenden Schutz. Die schematische Bindung des Sub-Processing an die vorgängige schriftliche Zustimmung des Verantwortlichen wäre in der Praxis hinsichtlich bestehender Auftragsbearbeitungen nur mit grösstem Aufwand umsetzbar. Zudem ist nicht nachvollziehbar, wieso dem Verantwortlichen ein (grundloses) Einspruchsrecht eingeräumt wird. Es handelt sich hier um einen unverhältnismässigen Eingriff in die Vertrags- und Wirtschaftsfreiheit. Nehmen wir als Beispiel ein Marketing-Unternehmen, das für seine Geschäftskunden Mailings zuhanden derer Kunden erstellt/versendet, also als Auftragsbearbeiter tätig ist. Möchte dieses Marketing-Unternehmen seine IT-Infrastruktur an einen Dritten auslagern, könnte dies von Gesetzes wegen am Einspruch eines einzigen seiner Geschäftskunden scheitern. Dies ist in einer digitalisierten und hochspezialisierten Welt praxisfremd. Vorstellbar wäre allenfalls eine Regelung, wonach der Auftragsbearbeiter auf Verlangen des Verantwortlichen eine Liste mit seinen (Sub-)Auftragsbearbeitern zur Verfügung stellt (was im Lichte der Dokumentationspflicht ohnehin angebracht erscheint). Es steht den Parteien frei, vertraglich weitergehende Einschränkungen festzulegen. Der Artikel ist weiter auch sonst systemfremd. Die Auftragsbearbeitung als solche ist unter den Voraussetzungen

					von Art. 7 Abs. 1 und 2 VE-DSG ohne weitere Genehmigung durch die betroffenen Personen zulässig. Warum die Subauftragsbearbeitung einer strengeren Regelung unterstellt werden soll, ist nicht ersichtlich. Richtigerweise sollten Art. 7 Abs. 1 und 2 VE-DSG für weitere Unterauftragsbearbeiter einfach analog gelten. Falls also der Verantwortliche seine Zustimmung verweigern würde, müssten bestehende Auftragsbearbeitungen vorzeitig beendigt werden, was zu erheblichen Mehrkosten der Leistungserbringung führen kann. Auch für künftige Auftragsbearbeitungen bringt diese Norm unnötigen Overhead bei den Auftragsbearbeitern und damit letztlich Mehrkosten bei den Verantwortlichen. Art. 7 Abs. 3 VE-DSG ist deshalb ersatzlos zu streichen.
swissICT	DSG	Div.	Div.		**Auftragsdatenbearbeitung / Erweiterte Pflichten des Auftragsbearbeiters** Die Pflichten des Auftragsbearbeiters werden im VE-DSG gegenüber dem Status Quo erheblich ausgeweitet. Dabei wird der Auftragsbearbeiter teils alleine und teils kumulativ, alternativ oder subsidiär zum Verantwortlichen in die Pflicht genommen. Hierbei ist nicht völlig klar, ob die sprachliche Unterscheidung jeweils bewusst getroffen wurde (z.B. alternative Pflicht bei der Datenschutz-Folgenabschätzung in Art. 16 VE-DSG, kumulative Pflicht hinsichtlich Privacy by Design und Privacy by Default in Art. 18 VE-DSG). Während die kumulative Verpflichtung des Auftragsbearbeiters im Rahmen von Art. 11 Abs. 1 VE-DSG (Datensicherheit) und Art. 19 Bst. a VE-DSG (Dokumentation) sachgerecht erscheint, ist sie bei Art. 18 VE-DSG zumindest in Bezug auf Privacy by Default abzulehnen, handelt es sich hierbei doch um eine inhärente Pflicht des Verantwortlichen, die der Auftragsbearbeiter gar nicht wahrnehmen kann. Auch die kumulativen Pflichten des Auftragsbearbeiters gemäss Art. 19 Bst. b VE-DSG gehen zu weit; hinsichtlich der Information über Verletzungen des Datenschutzes besteht gar ein Widerspruch zu Art. 17 Abs. 4 VE-DSG, wonach der Auftragsbearbeiter (nur) den Verantwortlichen über eine unbefugte Datenbearbeitung zu informieren hat.

					Auch die alternative Verpflichtung ergibt bei einzelnen Bestimmungen keinen Sinn: So kann die Mitteilung einer Datenbekanntgabe ins Ausland in Ausnahmefällen gemäss Art. 6 Abs. 2 VE-DSG konsequenterweise nur durch den Verantwortlichen erfolgen, weil nur jener sich auf die entsprechenden Ausnahmetatbestände gemäss Art. 6 Abs.1 VE-DSG berufen kann. Die überschiessende Ausweitung der Pflichten des Auftragsbearbeiters ist auch deshalb als problematisch einzustufen, weil bei einem Verstoss gegen diese Pflichten auch der Auftragsbearbeiter unter die Sanktionsnorm gemäss Art. 51 VE-DSG fällt. Die dem Auftragsbearbeiter unter dem VE-DSG obliegenden Pflichten sollten deshalb auf das absolut Notwendige beschränkt werden und nur dort Anwendung finden, wo der Auftragsbearbeiter auch über die entsprechende Kompetenz und Möglichkeit in der Sache verfügt, um die Pflichten einzuhalten.
swissICT	DSG	8 und 9			Selbstregulierung ist besonders bei technikneutralen, aber dennoch techniknahen Regulierungen wichtig. Art. 8 und 9 VE-DSG werden deshalb ausdrücklich begrüsst. Dabei ist es zentral, dass die Wirtschaft einbezogen wird, wenn der EDÖB von sich aus Regelungen der guten Praxis ausarbeitet, wie das in Art. 8 Abs. 1 VE-DSG vorgesehen ist.
swissICT	DSG	12			**Kernanliegen: Ersatzlose Streichung des ganzen Artikels** Die Regelung von Art. 12 VE-DSG ist schwer verständlich und erscheint im VE-DSG als Fremdkörper. Soweit es sich bei Personendaten auch um Geschäftsdaten handelt, was die Regel ist, bestehen gemäss diversen andern einschlägigen Gesetzen (wie z.B. Buchführungsrecht gemäss OR, Steuerrecht, spezialgesetzliche Regelungen wie z.B. im Finanzmarktrecht zur Sicherstellung von Anlegerschutz, etc.) weitreichende legitime Dokumentations- und Archivierungspflichten, welche dem Kerngehalt von Art. 12 VE-DSG zuwiderlaufen. Nur schon deshalb bringt Art. 12 VE-DSG in dieser pauschalen Formulierung mit Wirkung für sämtliche Branchen und Konstellationen nichts und ist demzufolge ersatzlos zu streichen. Bei genauerem Betrachten fokussiert die Regelung wohl auf Daten einer verstorbenen Person auf **Social Media-Plattformen**. Dann sollte dies aber wenn schon in der Regelung auch explizit so eingeschränkt werden. Allerdings bringt die Regelung auch im Bereich Social Media keinen erkennbaren Mehrwert.

					Effektiv gehen beim Tod einer Person dessen Rechte qua **erbrechtlicher Universalsukzession** ohne Weiteres auf die Erben über (Art. 560 Abs. 1 ZGB). Gestützt auf diesen erbrechtlichen Übergang sämtlicher Rechte von Gesetzes wegen sind die Erben bereits ausreichend legitimiert, geeignete Massnahmen vorzukehren und z.B. die Löschung von Daten des Erblassers auf einer Social Media-Plattform zu verlangen. Die Regelung von Art. 12 VE-DSG ist somit weder nötig noch sinnvoll. Umgekehrt können die Erben per definitionem auch nicht mehr Rechte haben, als der Erblasser sie hatte. Art. 12 VE-DSG ist sogar kontraproduktiv, weil er eine Regelung aufstellt, welche zumindest nicht deckungsgleich ist mit etabliertem Erbrecht. Gleiches gilt mit Bezug auf Regelungen von Amts- und Berufsgeheimnissen in bereits bestehenden gesetzlichen Regelungen, für Banken z.B. nach Art. 47 BankG. Die pauschale Regelung, dass unter Art. 12 Abs. 3 VE-DSG Amts- und Berufsgeheimnisse generell nicht geltend gemacht werden können, kann so jedenfalls nicht stimmen. Tritt z.B. gemäss Vereinbarung der Erbengemeinschaft nur ein einzelner Erbe in die Rechtsstellung des Erblassers z.B. einer bestimmten Bank gegenüber ein, stehen nur diesem Erben sämtliche Rechte des Erblassers zu, während gegenüber allen andern Erben das Bankkundengeheimnis uneingeschränkt gilt. Nach alledem ist Art. 12 VE-DSG jedenfalls geeignet, statt der– heute nach Erbrecht bestehenden – Rechtssicherheit eher **Widersprüche zu bestehenden gesetzlichen Regelungen** zu produzieren. Aufgrund all dieser Argumente fordern wir die **ersatzlose Streichung von Art. 12 VE-DSG**. Stattdessen ist soweit sinnvoll zu überlegen, inwieweit gezielte spezialgesetzliche Regelungen z.B. in Ergänzung von Art. 28 ff. ZGB sinnvoll erscheinen. Nach dem Gesagten eher nicht.
swissICT	DSG	13			Die aktive Informationspflicht wird auf alle Personendaten ausgeweitet, was zu erheblichem Mehraufwand für die Unternehmen führen würde. Das ist abzulehnen. Die Informationspflicht sollte nur für besonders schützenswerte Personendaten und im Fall der Profilierung gelten. Wichtig ist ferner, dass die aktive Informationspflicht ausschliesslich bei der Beschaffung gilt, nicht bei jeder weiteren Bearbeitung und auch nicht bei weiteren Bekanntgaben an Dritte. So ist Art. 13 VE-DSG auch zu verstehen, wie sich aus Abs. 1 ergibt. Daran kann Abs. 3 VE-DSG nichts ändern. Sollte Abs. 3 VE-DSG dagegen so zu lesen sein, dass bei *jeder* Drittbekanntgabe erneut zu informieren ist, wäre eine solche Regel nicht praktikabel unbedingt abzulehnen.

					In den Erläuterungen sollte präzisiert werden, dass bei allfälligen Änderungen keine Nachinformation erfolgen muss.
swissICT	DSG	13	3		Vgl. zu Art. 13 oben.
swissICT	DSG	13	4		Art. 13 Abs. 4 VE-DSG ist konzeptionell falsch und muss gestrichen werden. Die Auftragsdatenbearbeitung basiert auf dem Konzept einer Privilegierung (Auftragsdatenbearbeiter ist der „lange Arm" des Verantwortlichen; alles was der Verantwortliche darf, kann er auch durch einen Auftragsdatenbearbeiter ausführen lassen). Art. 7 VE-DSG geht dementsprechend davon aus, dass eine Auftragsdatenbearbeitung nur dann vorliegt, wenn eben die dort genannten Voraussetzungen (Vertrag, Sicherheitsbestimmungen, Weisungsgebundenheit, namentlich Verwertungsverbot zu eigenen Zwecken) erfüllt sind. Wenn sie erfüllt sind, liegt die privilegierte Situation „Auftragsdatenbearbeitung" vor. Sind sie nicht erfüllt, greift auch die Privilegierung nicht; und es liegt ein Fall der „Bekanntgabe" vor. Mit anderen Worten: Die Informationspflicht bei Auslagerung – also Art. 13 Abs. 4 VE-DSG – ist systemwidrig und steht quer in der Landschaft des VE-DSG, das eine gesteigerte Risikosituation grundsätzlich nur bei der Bekanntgabe sieht. Bereits Art. 7 Abs. 4 VE-DSG zeigt (wie das bisherige Recht), dass jedenfalls der IT-Dienstleister nicht als Dritter zu bezeichnen ist. Das DSG verpflichtet den Verantwortlichen bereits zur Einhaltung des DSG und allen weiteren Massnahmen (Auswahl des Dienstleisters, Sicherheit, etc.) – genau gleich, wie wenn er selber die IT betreibt. Wenn er diesbezüglich Fehler macht, können die Behörden sanktionieren (neu allenfalls sogar strafrechtlich). Die betroffene Person kann von der vorgeschriebenen Information nicht profitieren. Im Gegenteil, die Mitteilungspflicht würde implizit denjenigen, der seine IT selber betreibt (auch wenn er dazu die notwendigen Kompetenzen nicht hat), als sicherer darstellen als denjenigen, der diese Aufgaben einem Experten überlässt. Die Bestimmung ist also auch sachlich falsch, geradezu gegenläufig zu den Interessierten der betroffenen Person.
swissICT	DSG	14			[siehe unten bei Art. 21]

swissICT	DSG	15			**Kernanliegen: Präzisierung der Pflichten nach Art. 15 VE-DSG** Die Informationspflicht und das Äusserungsrecht nach Art. 15 Abs. 1 und 2 VE-DSG (zu letzterem s. unten) gelten, sofern eine automatisierte Einzelfallentscheidung „rechtliche Wirkungen oder erhebliche Auswirkungen“ auf die betroffene Person hat. Diese beiden Tatbestandselemente sind sehr vage, was zu Rechtsunsicherheit führt. Sie sollten daher im Text von Art. 15 Abs. 1 VE-DSG eingeschränkt werden. Zumindest wäre im Erläuternden Bericht bzw. der Botschaft festzuhalten, dass die Schwelle für „rechtliche Wirkungen“ und für „erhebliche Auswirkungen“ jeweils hoch ist und dass die Verweigerung eines Vertragsschlusses zumindest im Regelfall keine „rechtliche Wirkung“ hat (weil i.d.R. kein Rechtsanspruch auf den Abschluss eines Vertrags besteht und seine Verweigerung daher nicht in eine Rechtsstellung eingreift). Andernfalls droht eine Ausweitung der ohnehin weitgehenden Pflichten nach Art. 15 Abs. 1 und 2 VE-DSG auch auf Bagatellentscheidungen.
swissICT	DSG	15	2		**Kernanliegen: Ersatzlose Streichung des Äusserungsrechts (Art. 15 Abs. 2 VE-DSG).** Ein zentraler Punkt der Digitalisierung ist die Automatisierung. Gerade durch Automatisierung lassen sich Effizienzgewinne und damit einhergehend Aufwandreduktionen erzielen, welche im heutigen wirtschaftlichen Umfeld enorm wertvoll, wenn nicht gar unabdingbar geworden sind. Zudem wirken sie sich auch positiv für die Kunden aus, z.B. durch tiefere Preise. Automatisierte Entscheide bringen gegenüber manuellen Entscheidungsprozessen zudem erhebliche Vorteile für Anbieter und Kunden mit sich (Objektivität der Entscheidung, geringere Kosten, schnellere Prozesse). Es ist deshalb nicht einzusehen, warum vollautomatisierte Entscheide durch die Datenschutzgesetzgebung faktisch verboten werden sollten. Diese Technophobie ist unbegründet, und sie widerspricht auch dem Ziel einer technikneutralen Regelung. Das in Art. 15 Abs. 2 VE-DSG neu vorgeschlagene Recht einer betroffenen Person, sich zu einer automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern („Anhörungspflicht“), stufen wir vor diesem Hintergrund als wettbewerbs- und auch innovationsbehindernd ein. Darüber hinaus ist dieses Recht aber auch schlicht unnötig, insbesondere angesichts der ebenfalls neu eingeführten Pflicht, die betroffene Person darüber zu informieren, wenn eine automatisierte Einzelentscheidung gefällt wurde (Abs. 1 von Art. 15 VE-DSG). Unabhängig davon quasi „auf

					Vorrat“ zu informieren produziert demnach keine zusätzliche Transparenz, sondern generiert lediglich unnötigen zusätzlichen Administrativaufwand. Zudem ist zu befürchten, dass die Einführung einer Pflicht zur „Äusserung“ in der Praxis zu einer Begründungspflicht führt und letztlich die Vertragsfreiheit eines Unternehmens erheblich einschränkt. Das ist ein konsumentenschützerisches Anliegen, das nicht ins Datenschutzrecht gehört. SwissICT setzt sich deshalb vehement für eine ersatzlose Streichung der Äusserungsrechts von Art. 15 Abs. 2 VE-DSG ein. Die Relevanz bestimmter Daten für die Richtigkeit von Entscheidungen und der Grad der Wichtigkeit von automatisierten Entscheidungen i.S.v. Art. 15 VE-DSG kann von Branche zu Branche ferner massiv unterschiedlich sein. Daraus ergibt sich, dass eine generelle Regelung für die gesamte Wirtschaft jedenfalls über das Ziel hinausschiesst. Nicht zum Vornherein abwegig ist es demgegenüber, soweit nötig für einzelne ganz bestimmte branchenspezifische Datennutzungen in einschlägigen Spezialgesetzen oder in Empfehlungen der guten Praxis (Art. 9 VE-DSG) eine angemessene Regelung zu treffen, welche den Besonderheiten der betreffenden Branche gebührend Rechnung trägt. Folgerichtig ist auch der entsprechende Abschnitt in Art. 20 Abs. 3 VE-DSG zu streichen. Die Information darüber, wie bestimmte Entscheide zustande kommen, gehört zum Geschäftsgeheimnis eines Unternehmens. Eine solche Informationspflicht ist demnach, insbesondere in der aktuell vorgesehen, detaillierten Form gemäss Art. 20 Abs. 3 VE-DSG, klar unverhältnismässig. So ist zum Beispiel im Finanzbereich die Einschätzung von Ausfallrisiken bei der Kreditvergabe ein wichtiges, differenzierendes Know-How eines Finanzdienstleisters. Die Auskunft über die für diese Einschätzung genutzten Daten und deren Gewichtung führt zu einer Replizierbarkeit dieser Einschätzung und damit zur Aufgabe dieses Geschäftsgeheimnisses. Offenlegungspflichten solcher Art würden im Ergebnis jede Innovationskraft der Wirtschaft abtöten, da der dafür eingesetzte Aufwand nicht angemessen geschützt werden könnte. Sollte dem Streichantrag wider Erwarten nicht gefolgt werden, müsste jedenfalls vorab Art. 20 Abs. 3 VE-DSG als dort – unter dem allgemeinen Auskunftsrecht – sachfremde Regelung gestrichen und mit Art. 15 VE-DSG zu einer in sich stimmigen Gesamtlösung

					verbunden werden. Dabei wäre die Regelung – entsprechend dem richtigen Ansatz der DSGVO, mit welchem der VE-DSG äquivalent zu sein hat – auf schwere Fälle zu begrenzen, d.h. auf solche mit erheblichen Auswirkungen auf die betroffene Person. Sodann wäre klarzustellen, dass jedenfalls eine einmalige angemessene Information ohne ausdrückliche Einwilligung im Sinne der Gesetzessystematik ausreichend ist. Dadurch wird auch das in Art. 20 Abs. 3 VE-DSG vorgesehene Auskunftsrecht über automatisierte Einzelfallentscheidungen obsolet. Die Kunden können zudem bis zu einem gewissen Grad selbst entscheiden, ob sie zu einem Anbieter wollen, der vollautomatisierte Entscheide trifft oder zu einem Anbieter, der zusätzlich oder vollständig auf die Arbeitskraft natürlicher Personen setzt. Diese Grundentscheidung mit Bezug auf das Geschäftsmodell spiegelt sich regelmässig auch in unterschiedlichen Preisen wieder. Auf Art. 20 Abs. 3 kommen wir nochmals zurück (s. unten).
swissICT	DSG	16			Die Regelung der Datenschutz-Folgenabschätzung („DSFA“) im Vorentwurf ist an sich überflüssig. Die Forderung von Art. 8bis der revidierten Konvention 108, bei geplanten Datenbearbeitung die Risiken einzuschätzen, wird durch Art. 11 des Vorentwurfs (Datensicherheit) bereits erfüllt. swissICT wendet sich dennoch nicht gegen eine eigene gesetzliche Regelung der DSFA. Die Pflicht, eine Datenschutz-Folgenabschätzung durchzuführen, ist im VE-DSG jedoch viel zu weit gefasst. Art. 16 ist wie folgt neu zu fassen (vgl. die folgenden einzelnen Bemerkungen): *1 Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem <u>hohen</u>~~erhöhten~~ Risiko für die Persönlichkeit ~~oder die Grundrechte~~ der betroffenen Person, so muss der Verantwortliche ~~oder der Auftragsbearbeiter~~ vorgängig eine Datenschutz-Folgenabschätzung durchführen.* *2 Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit ~~oder die Grundrechte~~ der betroffenen Person*

					sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit ~~oder der Grundrechte~~ der betroffenen Person zu verringern. *3 Der Verantwortliche ~~oder der Auftragsbearbeiter~~ benachrichtigt den Beauftragten über das Ergebnis der Datenschutz-Folgenabschätzung und die vorgesehenen Massnahmen, sofern trotz der vorgesehenen Massnahmen hohe Restrisiken für eine Verletzung der Persönlichkeit der betroffenen Person vorauszusehen sind.* *4 Hat der Beauftragte Einwände gegen die vorgesehenen Massnahmen, so teilt er dies dem Verantwortlichen ~~oder dem Auftragsbearbeiter~~ innerhalb von ~~drei Monaten~~ einem Monat nach Erhalt aller erforderlichen Informationen mit.*
swissICT	DSG	16	1		**Kernanliegen: Die Bestimmung muss präzisiert werden, und der Hinweis auf die Grundrechte der betroffenen Personen ist zu streichen.** Der Ausdruck „erhöhtes Risiko“ in Abs. 1 ist viel zu unbestimmt. Er geht zudem über die europäischen Vorgaben hinaus: Art. 35 f. DSGVO und Art. 27 Ziff. 1 der Schengen-Richtlinie verlangen eine Datenschutz-Folgenabschätzung jeweils nur bei einem „hohen“ Risiko. Der VE-DSG ist entsprechend anzupassen. Ohne eine solche Anpassung müsste jede Bearbeitung, die in irgendeiner Hinsicht ein Risiko mit sich bringt (schon jede Übermittlung ins Ausland) zu einer Datenschutz-Folgenabschätzung und einer Meldung an den EDÖB führen (schon wegen des Sanktionsrisikos). Dies würde hohe Kosten verursachen, denen kein Mehrwert gegenüber steht. Es ist zudem falsch, von einem Risiko für „die Grundrechte“ der betroffenen Personen zu sprechen. Das entspricht zwar mehr oder weniger der Regelung der DSGVO. Das europäische Recht kennt aber eine direkte Drittwirkung der Grundrechte, die dem schweizerischen Recht fremd ist. Wenn Art. 16 VE-DSG vom Risiko für Grundrechte spricht, würde dies eine konzeptionelle Änderung bedeuten. Das ist abzulehnen: Es ist nicht Aufgabe privater Datenbearbeiter, die Grundrechte betroffener Personen zu schützen, soweit diese Grundrechte nicht in den einzelnen Anforderungen des DSG

					Ausdruck gefunden haben. Dazu kommt, dass völlig unklar ist, um welche Grundrechte es geht und welche Risiken dabei relevant wären. Schliesslich spricht Art. 16 Abs. 1 VE-DSG davon, dass „der Verantwortliche *oder* der Auftragsbearbeiter“ verpflichtet sind, die Datenschutz-Folgenabschätzung durchzuführen. Diese Formulierung kann nur bedeuten, dass die Pflicht den Verantwortlichen trifft, dieser aber befugt ist, die Durchführung der Datenschutz-Folgenabschätzung dem Auftragsbearbeiter zu übertragen. Die Formulierung ist aber missverständlich und daher zu präzisieren (s. oben).
swissICT	DSG	16	3		**Kernanliegen: Beschränkung der Meldepflicht auf Fälle hoher Restrisiken; Kürzung der Reaktionsfrist des EDÖB.** Viel zu weit geht auch die Meldepflicht an den EDÖB. Nach der vorgeschlagenen Regelung ist der EDÖB über jede Datenschutz-Folgenabschätzung zu informieren. Das ist strikt abzulehnen: • Jede Datenschutz-Folgenabschätzung melden zu müssen, stellt einen massiven Eingriff in die Geheimsphäre der Unternehmen dar. • Den Unternehmen würde durch eine solche Meldepflicht ein Anreiz gesetzt, im Zweifel keine Datenschutz-Folgenabschätzung durchzuführen. Das wäre kontraproduktiv. • Wenn jede Datenschutz-Folgenabschätzung meldepflichtig ist, wird der EDÖB von Meldungen überflutet. Er kann auf die zahlreichen Meldungen von Datenschutz-Folgenabschätzung nicht reagieren. Eine unterschiedslose Meldepflicht führt nur zu bürokratischen Leerläufen ohne Nutzen. • Selbst das europäische Recht verlangt nicht, die Aufsichtsbehörden von jeder Datenschutz-Folgenabschätzung zu informieren. Art. 36 Abs. 1 DSGVO verlangt eine Meldung im Gegenteil nur dann, wenn die Datenschutz-Folgenabschätzung ergibt, dass trotz der vorgesehenen Massnahmen ein hohes Risiko verbleibt. Art. 36 Abs. 1 DSGVO ist zwar unklar formuliert, doch ergibt sich dies eindeutig aus den Erwägungsgründen der DSGVO. Auch die Reaktionszeit des EDÖB von drei Monaten ist viel zu lange. Wenn Unternehmen drei Monate auf eine Antwort des EDÖB warten müssen, führt dies zu erheblichen Verzögerungen und wirkt massiv innovationshemmend. Im Fall einer Meldung hat der EDÖB ausschliesslich zu prüfen, ob die

					vorgeschlagenen Massnahmen ausreichend sind. Dafür genügt ein Monat. Dies insbesondere deshalb, weil der EDÖB diese Frist durch Nachfragen laufend verlängern kann.
swissICT	DSG	17	1		**Kernanliegen: Die Meldepflicht gegenüber dem EDÖB ist einzuschränken.** Die Pflicht sollte auf hohe Risiken eingeschränkt werden; insbesondere aufgrund der vorgesehenen Sanktionierung (vgl. Art. 50 Abs. 2 lit. d VE-DSG). Die Meldung an den EDÖB muss „unverzüglich“ erfolgen. Das ist so zu verstehen, dass die Meldung ohne unbegründete Verzögerung erfolgen sollte, nachdem der Verantwortliche vom meldepflichtigen Vorgang ausreichende Kenntnis hat, um das Risiko einschätzen zu können. In diesem Sinne ist dem Erläuternden Bericht beizupflichten, der den Ermessensspielraum des Verantwortlichen anspricht. Aus Abs. 1 VE-DSG ist nicht ersichtlich, ob dem Beauftragten lediglich die Datenschutzverletzung oder bestimmte / weitergehende Informationen hierzu mitzuteilen sind (vgl. demgegenüber Art. 33 Abs. 3 DSGVO). Das ist zu präzisieren. Unklar ist zudem, ob auch Bagatellmeldungen darunter fallen; diese sind klar auszuschliessen bzw. es sollten nur jene Datenschutzverletzungen meldepflichtig sein, die (i) relevanten Risiken (ii) mit gewisser Eintrittswahrscheinlichkeit verbunden sind.
swissICT	DSG	17	2		**Kernanliegen: Die Meldepflicht gegenüber den betroffenen Personen ist zu präzisieren.** Es ist nicht klar, wann und mit welchem Inhalt die betroffene Person genau zu informieren ist. Nach DSGVO 34 ist die betroffene Person nur zu informieren, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person hat. Dies sollte im VE-DSG entsprechend angepasst werden.
swissICT	DSG	17	4		Die Informationspflicht des Auftragsbearbeiters zuhanden des Verantwortlichen sollte erst dann ausgelöst werden, wenn der Auftragsbearbeiter von einer Verletzung Kenntnis hat. Art. 17 Abs. 4 sollte daher wie folgt formuliert werden: *4 Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung, sobald er davon Kenntnis hat.*

swissICT		18			Die Formulierung von Art. 18 VE-DSG ist unklar und geht über die in Art. 25 DSGVO enthaltenen Anforderungen hinaus. swissICT vertritt zudem die Auffassung, dass Art. 18 VE-DSG systematisch zu Art. 11 VE-DSG gehört bzw. bereits durch das geltende Recht gedeckt ist Die Bestimmung sollte gestrichen und in Art. 11 VE-DSG integriert werden, wobei nicht über die Anforderungen der DSGVO hinauszugehen ist.
swissICT	DSG	20	1		**Kernanliegen: Massvolle Anwendung des Auskunftsrechts und Schutz vor Missbrauch.** Das allgemeine Auskunftsrecht ist im Kern unbestritten. Die Ausweitung des Auskunftsrechts auf sämtliche Datenbearbeitungen und überdies auf hängige Verfahren (vgl. Art. 2 Abs. 3 VE-DSG) ist jedoch unverhältnismässig. Dies gilt umso mehr, als gemäss geltender Schweizer Rechtsprechung kein Auskunftsersuchen je rechtsmissbräuchlich sein kann, weil selbst ein untergeordnetes Datenschutzinteresse ausreicht, um einen Auskunftsanspruch zu bejahen. Die Anknüpfung am bisher bewährten System der Datensammlung wäre sachgerechter und würde den betroffenen Personen ausreichenden Schutz bieten. Schliesslich ist dem zunehmenden Missbrauch des Auskunftsrechts für datenschutzfremde Zwecke ein Riegel zu schieben. Die Vergangenheit hat leider gezeigt, dass datenschutzrechtliche Begründungen viel zu leicht vorgeschoben werden können, um eine kostenlose Beschaffung von Beweismitteln durchzusetzen. Die Anzahl querulatorischer, kosten- und ressourcenintensiver Fälle zu reinen Schikanezwecken hat deshalb stark zugenommen. Aus diesen Gründen ist auch der Ansatz falsch, das Auskunftsrecht generell kostenlos auszugestalten. Damit wird mit dem Verursacherprinzip ein Grundsatz verletzt, welcher ansonsten in der Rechtsordnung generell gilt. Dementsprechend ordnet auch die DSGVO keine allgemeine Kostenlosigkeit an (Art. 12 Ab. 5 DSGVO). Die von Art. 20 Abs. 1 VE-DSG angeordnete pauschale Kostenlosigkeit der Auskunft ist deshalb **nicht äquivalent** und demzufolge ersatzlos zu streichen und stattdessen ein angemessener Unkostenbeitrag vorzusehen. Zur effizienten Bekämpfung von Rechtsmissbrauch ist die Regelung überdies dahingehend auszugestalten, dass – innerhalb des Anwendungsbereichs von Rechtsmissbrauch – bei besonders aufwendigen Verfahren nach vorgängiger

					Abmahnung der betroffenen Person kein maximales Kostendach mehr gilt, sondern über den angemessenen Unkostenbeitrag hinaus die effektiven Kosten geltend gemacht werden dürfen. Dies ist mit rechtsstaatlichen Grundsätzen durchaus vereinbar bzw. von ihnen geradezu gefordert, muss es doch auch darum gehen, den Auskunftspflichtigen vor uferlosem Aufwand aufgrund von klarem Rechtsmissbrauch zu schützen. In der Formulierung von Art. 20 Abs. 1 VE-DSG ist deshalb das Wort **„kostenlos" ersatzlos zu streichen** (vgl. im Übrigen zu Art. 21 VE-DSG). Alternativ wäre analog Art. 12 Abs. 5 lit. a DSGVO dem Bundesrat die Kompetenz einzuräumen, die Ausnahmen der Kostenlosigkeit auf Verordnungsstufe festlegen zu können. Ohne diese Ermächtigung können keine Ausnahmebestimmungen Eingang in die Verordnung finden (vgl. zum Rechtsmissbrauch und den Verfahrenskosten ferner zu Art. 21 VE-DSG.
swissICT	DSG	20	2	b	Wir empfehlen entsprechend der bewährtem heutigen Regel die Präzisierung, dass die Auskunft nur die Kategorien der bearbeiteten Personendaten beinhalten muss. Dies entspricht auch Art. 15 lit. b DSGVO.
swissICT	DSG	20	2	e	Im Rahmen der allgemeinen Auskunftspflicht darf die geforderte Information über automatische Einzelfallentscheidungen nicht eine detaillierte Auflistung aller in der Vergangenheit ausgeführten automatischen Einzelfallentscheidungen verlangen. Vielmehr sollte eine allgemeine Information über auomatisierte Einzelfallentscheidungen genügen. Aus diesem Grund ist auch Art. 20 Abs. 3 zu streichen (vgl. sogl.).
swissICT	DSG	20	2	f	Wir erachten es als ausreichend, wenn die Herkunft der Personendaten dann angeben werden muss, wenn die Daten nicht bei der betroffenen Person selbst erhoben wurden. Dies entspricht Art. 15 Abs. 1 lit. g DSGVO. Anpassungsvorschlag: *f. Die verfügbaren Informationen über die Herkunft der Personendaten, falls diese nicht bei der betroffenen Person erhoben wurden.*

swissICT	DSG	20	2	g	„Empfänger“ der Daten schliesst auch Auftragsdatenbearbeiter ein. Es ist nicht praktikabel, sämtliche Auftragsbearbeiter inkl. Identität und Kontaktdaten zu nennen. Die DSGVO verlangt denn auch nur die Angabe von Kategorien von Empfängern.
swissICT	DSG	20	3		**Kernanliegen: Streichung der besonderen Auskunftspflicht bei Entscheidungen in Art. 20 Abs. 3 VE-DSG** Ein individuelles Auskunftsrecht mit Bezug auf Ergebnis, Zustandekommen und Auswirkungen jeder Entscheidung ist aus grundsätzlichen Überlegungen abzulehnen. Das Auskunftsrecht muss sich wie nach geltendem Recht auf kategorielle Informationen beschränken (wie bspw. die Auskunft zu Weitergaben an Dritte, bei denen weder alle Weitergaben noch alle Empfänger zu nennen sind, sondern nur die Kategorien der Empfänger). Die vorgeschlagene Auskunftspflicht bei Entscheidungen nach Art. 20 Abs. 3 VE-DSG würde die Auskunftspflicht daher enorm ausweiten. Sie wäre entsprechend massiv aufwendiger als bisher, ohne dass damit ein besserer Schutz der betroffenen Personen erreicht würde. Sehr viele Entscheidungen liegen ferner im Rahmen dessen, was für die betroffenen Personen ohne weiteres erkennbar ist (vgl. Art. 4 Abs. 3 VE-DSG). Die vom VE-DSG vorgeschlagene Regelung geht zudem klar über den von den EU-Anforderungen gesetzten Rahmen hinaus (vgl. Art. 15 Abs. 1 lit. h DSGVO). Dies stellt einen kontraproduktiven Swiss Finish dar, welcher dem Regulierungsziel der Äquivalenz entgegen steht und deshalb abzulehnen ist. Der von Art. 20 Abs. 3 Halbsatz 2 VE-DSG geforderte Umfang des Auskunftsrecht („Informationen über Ergebnis, Zustandekommen und Auswirkungen der Entscheidung“) ist mit Blick auf die anderweitig im VE-DSG bereits bestehenden weitreichenden Informationspflichten ferner weder sinnvoll noch nötig. Er produziert ohne Mehrwert z.B. in Form von mehr Transparenz unnötigen zusätzlichen Administrativaufwand. Eine derart weitgehende Auskunftspflicht ist datenschutzrechtlich nicht zu rechtfertigen. Insbesondere die Anwendung auf jede Art von Entscheidungen – nicht nur auf automatisierte Einzelfallentscheidungen – ist viel zu weitgehend. Sie könnte ausserdem zu einer Offenlegung von Geschäftsgeheimnissen z.B. in Form von internen Entscheid- und Ablaufverfahren führen (dazu bereits oben zu Art. 15).

					Die Regelung würde schliesslich zu Unrecht eine Vermischung des allgemeinen Auskunftsrechts mit individuellen Auskünften zu Einzelfallentscheidungen produzieren. Auskünfte nach Art. 20 VE-DSG müssen in allgemeiner, übersichtlicher und leicht verständlicher Form erfolgen. Sie dürfen deshalb nicht mit einer Auflistung sämtlicher in der Vergangenheit durchgeführten individuellen Entscheidungen wie z.B. automatisierten Einzelfallentscheidungen ergänzt werden. Solches würde den Rahmen sprengen und wäre für den Adressaten nicht mehr verständlich, sondern im Gegenteil verwirrend. Deshalb ist Abs. 3 von Art. 20 VE-DSG hier systematisch falsch zugeordnet und gehört – wenn schon – zur gesamtheitlichen Regelung von Art. 15 VE-DSG. Zusammenfassend ist die Regelung von Art. 20 Abs. 3 VE-DSG in Art. 20 zu streichen und stattdessen in die Regelung von Art. 15 DSG zu integrieren. Auch diese Integration muss sich aber an die vorstehend und überdies zu Art. 15 VE-DSG skizzierten Grundsätze halten und sich insbesondere auf eine sehr generelle Darlegung der Funktionsweise automatisierter Einzelfallentscheide beschränken.
swissICT	DSG	20	5		Wir schlagen vor, den 2. Satz von Art. 20 Abs. 5 VE-DSG zu streichen.
swissICT	DSG	20bis (neu)			**Kernanliegen: Korrektur der Ausnahmetatbestände und Missbrauchsschutz** Die Ausnahmetatbestände von Art. 21 VE-DSG sind zu eng formuliert und inkonsistent. So ist nicht einzusehen, weshalb die Informationspflicht bei Unmöglichkeit und Unzumutbarkeit nur entfallen soll, soweit der Verantwortliche die betreffenden Daten nicht Dritten bekannt gibt (Art. 14 Abs. 4 lit. a VE-DSG). Das widerspricht auch der Regel, dass die Informationspflicht generell nicht nachzuholen ist, wenn dies nicht unmöglich oder unzumutbar ist (Art. 14 Abs. 5 VE-DSG). Richtigerweise muss die Informationspflicht immer entfallen, wenn die Information nicht möglich oder unzumutbar ist, wie es auch die DSGVO vorsieht (Art. 12 Abs. 5 lit. b DSGVO). Dies gilt umso mehr, als das Auskunftsrecht neu bei jeder Datenbearbeitung greift, da es keine Beschränkung mehr auf Datensammlungen geben wird. Nicht nachvollziehbar ist auch, weshalb die Informationspflicht nach gesetzlicher Vorschrift nur bei indirekter Beschaffung durch Dritte entfallen soll (Art. 14 Abs. 2 lit. a VE-DSG). Umso mehr muss

					die Informationspflicht bei direkter Beschaffung entfallen. Zudem ist abzulehnen, dass die Informationspflicht nur dann entfällt, wenn eine gesetzliche Vorschrift *dieses Entfallen* vorsieht (Art. 14 Abs. 3 lit. a VE-DSG). Richtig wäre, die Informationspflicht entfallen zu lassen, wenn und soweit die gesetzliche Vorschrift *die Bearbeitung* vorschreibt, denn dann besteht bereits gesetzliche Transparenz, so dass die Auskunft nicht mehr erforderlich ist. Dem Auskunftsverpflichteten muss sodann nach allgemeinen Rechtsgrundsätzen generell das Recht zustehen, das Auskunftsrecht unter Berufung überwiegender eigener Interessen einzuschränken oder sogar zu verweigern. Um dieser Regel griffige Konturen zu verleihen, sind – ohne Anspruch auf Vollständigkeit – typische Fallgruppen direkt im Gesetz aufzuführen. Das datenschutzrechtliche Auskunftsrecht dient der Beseitigung eines allfälligen Informationsgefälles zwischen betroffener Person und Auskunftspflichtigem. Die datenschutzrechtliche Begründung für das Auskunftsrecht fokussiert somit auf diejenigen Daten, welche die betroffene Person gar nicht kennt und aufgrund aller Umstände, z.B. mangels Erkennbarkeit (vgl. Art. 4 Abs. 3 VE-DSG), vernünftigerweise auch gar nicht kennen kann. Naturgemäss nicht im Fokus sind demzufolge Daten, welche die betroffene Person bereits kennt bzw. erhalten hat, z.B. in Form von Verträgen, Abrechnungen und Korrespondenzen aller Art. Dies ist schon deshalb richtig, weil es nicht Aufgabe des Auskunftspflichtigen sein kann, einer betroffenen Partei wiederholt immer wieder und sogar unter Strafandrohung dieselben Daten liefern zu müssen, nur weil die betroffene Person z.B. den Aufwand sparen will, diese bereits erhaltenen Daten z.B. in Form von Verträgen bei sich selbst in vernünftiger Form aufzubewahren. Ebenfalls nicht herauszugeben sind Daten, welche aufgrund gesetzlicher Pflichten zu erheben und/oder aus bestimmten Gründen der betroffenen Person nicht bekannt gegeben werden dürfen, z.B. wegen Vereitelungs- oder Kollusionsgefahr in Zusammenhang mit Abklärungen zur Verhinderung von Geldwäscherei, Terrorismusfinanzierung und Korruption. Selbstredend darf das datenschutzrechtliche Auskunftsrecht auch nicht dazu führen, dass – ebenfalls rechtlich geschützte – Geschäftsgeheimnisse (vgl. Art. 162 StGB) herausgegeben werden müssen. Nicht herausgabepflichtig sind überdies rein intern bearbeitete Daten.

					Der Auskunftsverpflichtete ist auch vor Auskunftsbegehren zu schützen, welchen klarer Rechtsmissbrauch zu Grunde liegt. Typische Fallgruppen klar rechtsmissbräuchlicher Geltendmachung des Auskunftsrechts sind aus Gründen der Rechtssicherheit direkt im Gesetzestext aufzuführen, insbesondere die Geltendmachung des Auskunftsrechts ohne sachlichen Grund oder die exzessive Geltendmachung des Auskunftsrechts mit häufiger Wiederholung, welche sachlich nicht nachvollziehbar ist. Zielführend ist es deshalb, direkt im Gesetz in Art. 21 VE-DSG aufzuführen, dass Daten der vorstehend skizzierten Art nicht herauszugeben sind. Auch in der DSGVO finden sich solche Ausnahmen und Einschränkungen. Zusammenfassend handelt es sich insbesondere um nachfolgend aufgeführte Daten. Formulierungsvorschlag: Art. 20bis VE-DSG: Nicht der Auskunftspflicht unterstehen folgende Datenkategorien: a) Bereits erhaltene Daten, welche die betroffene Person bereits erhalten hat, z.B. in Form von Verträgen, Abrechnungen und Korrespondenzen; b) aufgrund einer gesetzlichen Pflicht bearbeitete Daten, z.B. zur Verhinderung von Geldwäscherei, Terrorismusfinanzierung und Korruption; c) Daten, welche vom Auskunftspflichtigen als Geschäftsgeheimnisse qualifiziert werden; d) rein intern bearbeitete Daten; e) Daten über Drittpersonen; f) unter rechtsmissbräuchlichen Umständen herausverlangte Daten, insbesondere die Geltendmachung des Auskunftsrechts ohne erkennbaren sachlichen Grund oder mit häufiger, sachlich nicht nachvollziehbarer Wiederholung.
swissICT	DSG	21			Mit Blick auf die dargelegte Gefahr des Missbrauchs des Auskunftsrechts, namentlich der Zweckentfremdung zur Beweismittelausforschung, ist ein Mechanismus vorzusehen, der das Auskunftsrecht für die datenschutzfremde Beweismittelausforschung verhindert. Dafür wäre eine Kostenregelung sinnvoll, die sich bspw. am Rechtsschutzinteresse des Gesuchstellers orientiert. Falls datenschutzfremde Interessen überwiegen, könnte eine höhere Gebühr verlangt werden; im umgekehrten Fall

					wäre eine geringe Gebühr angezeigt (vgl. zu den Kosten einer Auskunft ferner zu Art. 20 Abs. 1 VE-DSG). Vorschlag für einen Art. 21 Abs. 3 VE-DSG: *Bei offensichtlich unbegründeten oder aus anderen Gründen missbräuchlichen Auskunftsersuchen kann der Verantwortliche für die Erteilung der Auskunft ein angemessenes Entgelt verlangen.* Eine analoge Formulierung drängt sich überdies auch bei Art. 14 in einem neuen Abs. 6 auf.
		44	3		Vorsorgliche Massnahmen im Bereich der Datenbearbeitung können massive 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.
swissICT]	DSG	45			**Kernanliegen: Einschränkung der Anzeigepflicht des EDÖB.** Die Pflicht des Beauftragten, Strafverfolgungsbehörden zu informieren, sollte nicht über Art. 58 DSGVO hinausgehen. Nach der DSGVO besteht ein Recht zur Anzeige, nicht jedoch eine Pflicht. Eine allgemeine Anzeigepflicht unterläuft die Informations- und Beratungspflicht des EDÖB nach Art. 49 lit. a VE-DSG: Wer mit einer Anzeige rechnen muss, wird sich hüten, in unklaren Fällen auf den EDÖB zuzugehen. Dies gilt ganz besonders angesichts der extrem weitgehenden Strafdrohung nach dem VE-DSG. Eine vertrauensvolle Zusammenarbeit mit dem EDÖB wird damit unmöglich.
swissICT	DSG	50 ff.			**Kernanliegen: konzeptionelle Änderung des Sanktionsmechanismus; angemessene Sanktionen gegen Unternehmen statt strafrechtliche Verfolgung Privater** Art. 50 ff. VE-DSG enthalten Strafbestimmungen gegen natürliche Personen. Dies steht im Gegensatz zu den entsprechenden europäischen Regelungen, die primär Sanktionen gegen Unternehmen vorsehen. Bei der Ausgestaltung des Sanktionssystems, namentlich Strafsanktionen oder Verwaltungssanktionen, lässt die DSGVO den Mitgliedstaaten Spielraum (vgl. Art. 83 Abs. 9 DSGVO sowie Erwägung 151 DSGV).

					Daher bleibt im Bereich der Aufsicht bzw. der Durchsetzung insofern ein wohl nicht unbeträchtlicher Handlungsspielraum, der eine wortwörtliche Übernahme der DSGVO nicht erforderlich macht. Verlangt wird ein der Sache nach **gleichwertiges Datenschutzniveau**, wobei im Bereich der Aufsicht/Sanktionierung im Wesentlichen wirksame, verhältnismäßige und abschreckende Sanktionen gefordert werden (Erwägung 152 DSGVO). Das Konzept des VE-DSG, zusammen mit der grossen Unbestimmtheit der Straftatbestände (dazu unten), führt somit zu einer nicht zu rechtfertigenden Bedrohung derjenigen Personen, die mit Personendaten umzugehen haben – und zwar gerade derjenigen Personen, die unternehmensintern die Einhaltung des Datenschutzes sicherstellen müssen und die durch das Datenschutzrecht deshalb zu schützen sind. Das ist auch deshalb verfehlt, weil Datenschutzverstösse viel eher an der unternehmensweiten Komplexität datenschutzrechtlicher Setups liegen (z.B. grenzüberschreitende Sachverhalte, zunehmender Trend zu Arbeitsteiligkeit, etc.) und nicht an individuellem Verschulden. Einzelne Personen zu bestrafen, wäre daher nicht sachgerecht. Es wäre zudem verfassungsrechtlich höchst bedenklich und ein klar überschiessender Swiss Finish, der massive Auswirkungen auf den Wirtschaftsstandort Schweiz hätte. Dieses verfehlte Konzept ist deshalb aufzugeben. Gleichzeitig stellt sich die Frage, ob das Strafrecht bei Datenschutzverstössen überhaupt das richtige Mittel sein kann (mit Ausnahme qualifizierter Verstösse wie etwa nach Art. 52 VE-DSG, der allerdings ebenfalls zu weit geht). Auch ein primäres Unternehmensstrafbarkeit ist daher zumindest kritisch zu hinterfragen, wenn nicht direkt abzulehnen: Ein eigentliches Unternehmensstrafrecht fehlt in der Schweiz (vgl. Art. 53 VE-DSG), und die punktuelle Unternehmensstrafbarkeit nach Art. 102 Abs. 1 StGB ist für Datenschutzverstösse gänzlich ungeeignet. Das zeigt ein Vergleich mit den Verstössen, die eine solche Strafbarkeit nach heutigem Recht auslösen können (z.B. Terrorismusfinanzierung, Korruptionsdelikte und Geldwäscherei) – Datenschutzverstösse können nicht mit organisierter Schwerkriminalität auf die gleiche Stufe gestellt werden. Die Ausgestaltung eines passenden verwaltungsrechtlichen Sanktionssystems für die Schweiz im Zusammenhang mit Verstössen gegen den Datenschutz bedarf aber zweifellos noch vertiefter Überlegungen. Aus den vorgenannten Gründen ist aber zu prüfen, ob nicht stattdessen Verwaltungssanktionen gegen fehlbare Unternehmen vorzusehen sind. Dies entspräche auch dem von der Mehrheit der europäischen Mitgliedstaaten gewählte Sanktionssystem.

					Dabei ist aber davon abzusehen, Verwaltungsverfahren anderer Bundesgesetze mit Verwaltungssanktionen ohne Weiteres und undifferenziert zu übernehmen. Hierzu folgende Ausführungen: Es fragt sich insbesondere, auf welche Weise die **Sanktionsbemessung** vorgenommen werden kann, dass sie nicht nur wirksam und abschreckend, sondern vor allem auch verhältnismässig ist (die Verhältnismässigkeit ist eine Anforderung der ERK 108 ebenso wie der DSGVO). Dabei ist zunächst eine angemessene **Obergrenze** für Unternehmensbussen festzulegen. Wichtig ist dabei, dass die Bussendrohung nicht kontraproduktiv wirkt. Die Obergrenze darf nicht so hoch ausfallen, dass ein Unternehmen in der Anwendung des Datenschutzrechts gelähmt wird. Insbesondere darf der (in der DSGVO sogar gestärkte) risikobasierte Ansatz nicht dadurch unterlaufen werden, dass Risiken durch übermässige Bussen untragbar werden. Denkbar wäre ein Höchstbetrag von CHF 500'000. Der Vollständigkeit halber sei nochmals erwähnt, dass die **Angemessenheitsentscheidung durch die EU-Kommission nicht verlangt, den Bussenrahmen der DSGVO zu übernehmen** (s. oben). Denkbar ist ferner auch ein unterschiedlich hoher Bussenrahmen je nach dem Sinn der verletzten Norm. Sollte man sodann bei der Sanktionsbemessung den Umsatz des betroffenen Unternehmens in Betracht ziehen wollen, so wäre jedenfalls sorgfältig abzuwägen, welcher Umsatz massgeblich ist – der Gesamtumsatz des betroffenen Bereichs, des betroffenen Projekts, der allfällig betroffenen Tochtergesellschaft oder des betroffenen Konzerns. Ebenso wichtig sind sodann die Kriterien der Sanktionsbemessung. Dabei muss eine angemessene Compliance des betroffenen Unternehmens erheblich mildernd ins Gewicht fallen: Datenschutzverstösse sind nicht zuletzt aufgrund der Vielzahl unbestimmter Begriffe und der Bedeutung von Wertungsentscheidungen und Risikoeinschätzungen nicht in jedem Falle vermeidbar. Sanktionswürdig ist daher nicht so sehr der Verstoss im Einzelfall – besondere Fälle vorbehalten –, sondern eine allenfalls ungenügende Prävention durch das Unternehmen. Bei einer Bemessung sollte ebenfalls eine allfällige proaktive Meldung einer Verletzung durch das Unternehmen unter Darlegung der Massnahmen berücksichtig werden. Hiermit wird durch die Revision verstärkt gewollte Kooperation zwischen dem Beauftragten und den Unternehmen Rechnung getragen.

					Wie erwähnt, sind ferner viele Pflichten des VE-DSG und damit auch die daraus abgeleiteten strafrechtlichen Tatbestände gemäss Art. 50 ff. VE-DSG zu wenig konkret. Art. 50 ff. VE-DSG erfüllen damit nicht die im Verfassungsrecht begründete Regel von „nulla poena sine lege (stricta, certa)". Vor diesem Hintergrund ist die Unbestimmtheit einer Mehrzahl der (Straf-)Tatbestände gem. Art. 50 f. VE-DSG äusserst bedenklich. Viele der Pflichten des VE-DSG und damit auch die daraus abgeleiteten Straftatbestände sind viel zu offen formuliert, dass es für ein Unternehmen auf Grund des erheblichen Auslegungsspielraumes schwierig sein wird zu verstehen, was es genau tun darf und was nicht. Aus diesem Grund sind die in dieser Stellungnahme an den betreffenden Stellen geforderten Präzisierungen umso wichtiger.

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
swissICT	6 Abs. 2 lit. c	Die Erläuterungen sollten klarstellen, dass unter „Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen" auch die „Abwehr" bzw. „Verteidigung" gegen Rechtsansprüche zu verstehen sind.
swissICT	13 Abs. 3	In den Erläuterungen sollte präzisiert werden, dass bei allfälligen Änderungen keine Nachinformation erfolgen muss.
swissICT	15 Abs. 1	Siehe obige Bemerkungen zu Art. 15 Abs. 1.