Geschäftsstelle

Wallstrasse 8
Postfach
CH-4002 Basel

Telefon 061 206 66 66
Telefax 061 206 66 67
E-Mail vskb@vskb.ch

Verband Schweizerischer Kantonalbanken
Union des Banques Cantonales Suisses
Unione delle Banche Cantonali Svizzere

Eidgenössisches Justizdepartement
EJPD
Herr Jonas Amstutz
Bundeshaus West
CH-3003 Bern

jonas.amstutz@bj.admin.ch

Datum 4. April 2017
Kontaktperson Lukas Aebi
Direktwahl 061 206 66 26
E-Mail l.aebi@vskb.ch

Stellungnahme der Kantonalbanken zur Revision des Datenschutzgesetzes

Sehr geehrte Damen und Herren

Sehr geehrter Herr Amstutz

Am 21. Dezember 2016 hat der Bundesrat die Vernehmlassung zur Revision des Datenschutzgesetzes eröffnet. Wir bedanken uns für die Gelegenheit, unsere Position und Überlegungen zum Revisionsentwurf im Rahmen des Vernehmlassungsprozesses einbringen zu können.

Zusammenfassung

Eine moderne, international kompatible und auf bewährten schweizerischen Regulierungsgrundsätzen aufbauende Datenschutzgesetzgebung ist im Sinne des Finanzplatzes Schweiz und der Kantonalbanken. Wir begrüssen daher das Revisionsvorhaben im Grundsatz. Dabei ist jedoch zentral, dass unverhältnismässige Belastungen für die Rechtsunterworfenen, die in keinem Verhältnis zum Schutzzweck des Gesetzes stehen, unbedingt vermieden werden.

Mit Blick auf den vorliegenden Revisionsentwurf besteht diesbezüglich noch viel Anpassungsbedarf. Die folgenden Kernanliegen, die in unserer Stellungnahme noch eingehender ausgeführt werden, sind für die Kantonalbanken von zentraler Bedeutung:

- Der Vorentwurf zum Datenschutzgesetz sollte sich an der revidierten Konvention 108 des Europarats und der Datenschutzgrundverordnung der Europäischen Union orientieren. Ein darüber hinaus gehender **«Swiss Finish» ist unnötig und schädlich** für den Wirtschaftsstandort Schweiz. So ist beispielsweise die Definition des sogenannten **«Profiling»** wesentlich breiter gefasst als die analoge Definition im Europäischen Recht. Dies ist nicht zielführend für eine Vereinheitlichung des Datenraumes in Europa und widerspricht damit der eigentlichen Absicht der Revision. Es gibt zahlreiche weitere Beispiele für unnötige und kontraproduktive Swiss finishes (vgl. dazu im Detail die nachfolgende Stellungnahme).
- Die zahlreichen verschärften und zusätzlichen Begründungs-, Anhörungs- und Informationspflichten führen für Unternehmen zu einer Flut von Meldungen an den Datenschutzbeauftragten und damit zu einem enormen, unverhältnismässigen und unnötigen Aufwand. Dies wirkt sich zudem wettbewerbs- und innovationsbehindernd aus.
- Sehr problematisch und **dezidiert abzulehnen sind die in Art. 50 ff. VE-DSG enthaltenen Strafbestimmungen**. **Diese setzen die Mitarbeiter von Bankinstituten einem enormen Haftungsrisiko bei der Datenbearbeitung aus.** Aus rechtsstaatlicher Sicht ebenso bedenklich sind die sehr offen formulierten Tatbestände, die einer Abkehr von den bewährten Grundsätzen der schweizerischen Strafrechtsdogmatik gleichkommen («nulla poena sine lege»). Auf die Strafbestimmungen ist daher zu verzichten, stattdessen sollten **angemessene verwaltungsrechtliche Sanktionskompetenzen** etabliert werden.
- Es gilt zu bedenken, dass Art. 19 des Bundesgesetzes über den internationalen automatischen Informationsaustausch in Steuersachen (AIAG) den meldepflichtigen Personen die Rechte nach DSG einräumt. Wenn nun im Rahmen der Datenschutzgesetzrevision die juristischen Personen explizit ausgenommen werden, stellt sich berechtigterweise die Frage**, ob damit juristische Personen nicht ihrer prozessualen Rechte beraubt werden.** Dies sehen wir kritisch.

- Der VSKB fordert ausserdem Mechanismen zur Verhinderung des Missbrauchs des Auskunftsrechts. **Im Sinne eines wirksamen Datenschutzes ist dieses so auszugestalten, dass es einzig zur Verfolgung von Datenschutzinteressen und nicht zur Beweismittelbeschaffung in Zivil- und Strafverfahren verwendet werden kann.** Es ist unserer Ansicht nach zudem falsch, das Auskunftsrecht kostenlos auszugestalten.
- Bei den angedachten Grundsätzen zur Bearbeitung von Personendaten ist darauf zu achten, **dass zentrale Bestimmungen des Geldwäschereigesetzes**, die eine Bank etwa dazu verpflichten, Informationen des Kunden und auffällige Transaktionen genau zu dokumentieren und aufzubewahren, **nicht unterlaufen werden**.

In der folgenden tabellarischen Übersicht sind unsere detaillierten Bemerkungen und Anliegen festgehalten:

Geschäftsstelle

Wallstrasse 8
Postfach
CH-4002 Basel

Telefon 061 206 66 66
Telefax 061 206 66 67
E-Mail vskb@vskb.ch

Verband Schweizerischer Kantonalbanken
Union des Banques Cantonales Suisses
Unione delle Banche Cantonali Svizzere

Detaillierte Bemerkungen zum Vorentwurf Datenschutzgesetz (VE-DSG)

Gesetz	Art.	Abs.	Bst.	Bemerkungen
DSG				**Vorbemerkung I:** Die Totalrevision des DSG sollte zwei Ziele verfolgen: • Anpassung an die revidierte Konvention 108 des Europarats (ERK 108) und • Beibehaltung der Anerkennung durch EU-Kommission, dass die Schweiz über einen angemessenen Datenschutz (Angemessenheitserklärung) verfügt. Letztere verlangt keine pauschale Übernahme der europäischen Datenschutz-Grundverordnung (EU-DSGVO). Für die Angemessenheitserklärung genügt es, grundlegende Garantien einzuhalten, beispielsweise die Rechtsstaatlichkeit oder die Existenz unabhängiger Aufsichtsbehörden. Die EU-DSGVO hält deshalb ausdrücklich fest, dass die Umsetzung der ERK 108 bei der Angemessenheitsbeurteilung ein wesentlicher Faktor ist. Illustriert wird dies dadurch, dass aus Sicht der EU-Kommission die Einhaltung der wenigen Regeln des US-EU Privacy Shields bekanntlich genügt, um einen angemessenen Datenschutz sicherzustellen. Vor diesem Hintergrund muss sich der **VE-DSG primär an der ERK 108 orientieren**. Darüber hinausgehende Regelungen können nur insofern sinnvoll sein, als sie helfen, einen einheitlichen Standard nach Massgabe der EU-DSGVO zu fördern. Damit wären Implementierungs- sowie Unterhaltskosten für

				Unternehmen, die in den Geltungsbereich beider Rechtsgrundlagen fallen und sämtliche Regelungen umsetzen müssen, auf ein verkraftbares Ausmass beschränkt. Dagegen wäre eine Verschärfung gegenüber der ERK 108 und der EU-DSGVO konzeptionell falsch, nicht notwendig und überdies **kontraproduktiv**, weil ein solcher **«Swiss Finish»** einen einheitlichen internationalen «Datenraum» zu Lasten der Schweiz verhindern und zulasten Schweizerischer Unternehmen wettbewerbsverzerrend wirken würde. Ein «Swiss Finish» kann daher zum Vornherein höchstens nur punktuell in Frage kommen, wo er eine wesentliche Erleichterung mit sich bringt.
DSG				**Vorbemerkung II:** Wir begrüssen, dass unter dem VE-DSG **Unternehmen keinen Datenschutz** mehr beanspruchen können. Damit wird Gleichlauf und somit Äquivalenz mit der EU-DSGVO hergestellt. Zu berücksichtigen ist allerdings die Tatsache, dass Unternehmen als rechtliche Fiktionen naturgemäss **zwingend durch natürliche Personen handeln** müssen. Bei jeder Datenbearbeitung durch Unternehmen entstehen deshalb per definitionem auch Daten von Mitarbeitenden des betreffenden Unternehmens, z.B. als Verfasser eines im Namen der Unternehmung erstellten Dokuments. Sämtliche solcher Daten von Mitarbeitenden dem Datenschutz zu unterstellen, wäre sachlogisch falsch und ein Widerspruch zur Tatsache, dass Unternehmen keinen Datenschutz mehr geniessen sollen. Deshalb ist **im Gesetz eine klare Abgrenzung** vorzunehmen. Diese muss statuieren, dass sämtliche Daten, welche über Mitarbeitende bei Ausübung oder bei Gelegenheit der geschäftlichen Tätigkeit für das Unternehmen entstehen, dem VE-DSG nicht unterstehen (vgl. Rosenthal/Jöhri, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 12 DSG N 24). Dementsprechend ist auch der künftig nicht mehr nötige Verweis in Art. 328b OR auf das DSG im gleichen Sinn anzupassen bzw. einzuschränken. Es gilt allerdings zu bedenken, dass Art. 19 des Bundesgesetzes über den internationalen automatischen Informationsaustausch in Steuersachen (AIAG) in Art. 19 den meldepflichtigen Personen die Rechte nach DSG einräumt. Wenn nun im Rahmen der Datenschutzgesetzesrevision juristische Personen explizit ausgenommen werden, stellt sich berechtigterweise die Frage, ob damit juristischen Personen nicht das Beschreiten des Rechtsweges im Rahmen des internationalen automatischen Informationsaustausches verwehrt wird. Aus Gründen der Adäquanz mit den europäischen Datenschutzregelungen ist die beste Lösung, nicht den Datenschutz wieder auf Unternehmen auszudehnen, sondern unter AIA Rechtsschutzmechanismen für Unternehmen ausserhalb des Datenschutzgesetzes zu etablieren.

DSG				**Vorbemerkung III:** Der VE-DSG sieht **zahlreiche verschärfte Prüf- und Meldepflichten** für Datenbearbeiter vor, die überdies einen erheblichen Eingriff in die Vertragsfreiheit bedeuten. Zu nennen sind insbesondere die Prüfung der Richtigkeit der Daten (Art. 4 Abs. 5 VE-DSG), die Meldepflichten bei Weitergabe von Daten ins Ausland (Art. 5 Abs. 3 Bst. c u. d i.V.m. Abs. 5 VE-DSG u. Art. 6 Abs. 2 i.V.m. Art. 6 Abs. 1 Bst. b-d VE-DSG), Informationspflichten, sofern Daten über einen Dritten beschafft werden (Art. 13 Abs. 5 VE-DSG), die Datenschutz-Folgeabschätzungen samt Meldepflicht (Art. 16 VE-DSG), umgehende Meldepflicht sämtlicher Datenschutzverletzungen (Art. 17 VE-DSG), Dokumentationspflichten (Art. 19a VE-DSG) und Pflicht zum Monitoring samt engem Zeitraum für allfällige Berichtigungen (Art. 19b VE-DSG). Das Gesamtpaket dieser Pflichten möge für spezifische Marketing-Dienstleister und Data-Miner angemessen sein, da sie im Rahmen eines eng begrenzten Geschäftsmodells typischerweise besonders sensible Datenbearbeitungen vornehmen. Für Datenbearbeiter, welche wie z.B. Banken ständig und in enormem Volumen Daten in Zusammenhang mit der Ausführung von Kundenaufträgen und aufgrund regulatorischer Vorgaben an zahllose Empfänger weitergeben müssen, ist die pauschale Anwendung solch strenger Regeln unbesehen der Sensibilität der betroffenen Daten nicht sachgerecht. Sie führen nicht zu besserem Datenschutz, sondern lediglich zu **enormem unnötigem Aufwand** und zu einer Flut von Meldungen an den Eidgenössischen Datenschutzbeauftragten (EDÖB). Ein derart intensives Paket von Pflichten ist umso bedenklicher, als es überdies auch noch weitgehenden strafrechtlichen Sanktionen unterstehen soll, welche erst noch entgegen etablierten Strafrechtsgrundsätzen sehr offen formuliert sind (vgl. Art. 50 ff. VE-DSG). Pflichten dieser Art sind deshalb nochmals in grundsätzlicher Form im Sinne einer Liberalisierung mit konsequentem Fokus auf die spezifischen **Bedürfnisse verschiedener Branchen** wie z.B. der Banken zu überarbeiten, damit die Wirtschaft nicht am Datenschutz «erstickt». Das neue DSG durchbricht gemäss VE ausserdem rechtsstaatliche Grundsätze, indem die gleiche Behörde Recht setzen und sprechen kann. Schliesslich enthält das Gesetz einige Auflagen, die in der Praxis nicht umsetzbar sind, was von einer mangelnden Prüfung auf die Umsetzbarkeit des Gesetzes zeugt.
DSG	1			**Kernanliegen: Berücksichtigung gesamtwirtschaftlicher sowie gesellschaftlicher Interessen bei der Bearbeitung von Personendaten**

				Die Bearbeitung von Personendaten ist Bestandteil und Voraussetzung nicht nur der erfolgreichen Digitalisierung der schweizerischen Wirtschaft und Gesellschaft, sondern überhaupt jeder wirtschaftlichen Tätigkeit. Infolgedessen muss das neue DSG bei der Bearbeitung von Personendaten auch gesamtwirtschaftliche und gesellschaftliche Interessen berücksichtigen. Dies würde auch der Zielsetzung der EU-DSGVO (Art. 1 Gegenstand und Zweck) entsprechen. Diese sieht neben dem Schutz natürlicher Personen auch den freien Verkehr von Personendaten als Zweck ausdrücklich vor. Zudem stünde die Berücksichtigung gesamtwirtschaftlicher sowie gesellschaftlicher Interessen im Einklang mit der Strategie des Bundesrates für eine digitale Schweiz. Demnach soll die Schweiz «Chancen der Digitalisierung in allen Lebensbereichen konsequent nutzen», von der „zunehmenden Digitalisierung profitieren», sich «als innovative Volkswirtschaft noch dynamischer entwickeln» und die «Wirtschaft soll sich im digitalen Raum möglichst frei entfalten können» (vgl. Medienmitteilung vom 20.04.2016 zur Strategie des Bundesrates für eine digitale Schweiz). Wir schlagen daher folgende Anpassung von Art. 1 VE-DSG (Zweck) vor: *Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden, und die Förderung des freien Verkehrs von Personendaten*
DSG	2	2	e	Zur Eindämmung des Missbrauchs und um die verfahrensrechtlichen Regeln gemäss den einschlägigen Verfahrensordnungen wie z.B. der ZPO nicht zu verwässern, fordern wir die **Wiedereinführung der Regel von Art. 2 Abs. 2 Bst. c DSG** mit Bezug auf sämtliche Zivil- und Strafverfahren (Nichtanwendbarkeit des DSG auf hängige Prozesse und anderer Verfahren) (vgl. im Einzelnen hinten zu Art. 20 Abs. 1 VE-DSG). Wäre dies nicht der Fall, so könnten über das DSG Daten beschafft werden, die im Rahmen der prozessualen Editionspflicht nicht herausgegeben werden müssten.
DSG	2	3		Es ist 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.
DSG	3		a	Definition der Personendaten: Nach heutiger Definition umfassen Personendaten alles, was irgendwie auf eine Person schliessen lässt. Im Rahmen des Bankgeschäfts sind somit sämtliche Belege, jeder Ausweis, jede Adressmutation etc. als Personendaten zu qualifizieren. Es ist zu beachten, dass die

				Pflichten zur Datenbearbeitung (beispielsweise Information bei Beschaffung oder Vernichtung von Daten) massiv ausgeweitet wurden. Mit der hier gewählten Definition ist es Banken unmöglich, den Pflichten dieses Gesetzes nachzukommen. Entsprechend wäre in der Definition zu unterscheiden, ob es sich um Personendaten grundsätzlicher Art handelt oder nicht. Eine Präzisierung der Begrifflichkeiten ist anzustreben. Wünschenswert wäre eine Unterscheidung, ob es sich um Personendaten grundsätzlicher Art handelt oder nicht.
DSG	3		c Ziff. 4	Die besonders schützenswerten biometrischen Daten sollten dahingehend präzisiert (eingeschränkt) werden, dass «zum Zweck» der Identifizierung ergänzt wird.
DSG	3		f	**Kernanliegen: Streichung des gegenüber der EU-DSGVO überschiessenden Swiss Finish und Beschränkung auf Personendaten sowie automatisierte Bearbeitung** Die Definition von «Profiling» ist zu breit und geht massiv weiter als die Definition gemäss der EU-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 einen partiellen Paradigmenwechsel im schweizerischen Datenschutzrecht dar, für den es keinen Grund gibt. Zudem umfasst «Profiling» gemäss VE-DSG 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. Richtigerweise darf «Profiling» nur diejenigen Daten erfassen, welche tatsächlich Rückschlüsse auf konkrete Personen zulassen, mithin nur Personendaten. Schliesslich ist eine Analyse bzw. Auswertung noch keine Datenbearbeitung, die sich per se negativ auf die Persönlichkeitsrechte der betroffenen Personen auswirkt. Richtigerweise ist der Begriff «Auswertung» durch «Bewertung» zu ersetzen, denn erst diese stellt einen schützenswerten Eingriff in die Persönlichkeitsrechte der betroffenen Personen dar. «Bewertung» umfasst eine Entscheidung mit Bezug auf eine einzelne betroffene Person, die sich auf eine Analyse bzw. Auswertung stützt. Die Anknüpfung an die Auswertung greift demnach zu weit. Art. 3 Bst. f ist deshalb wie folgt zu ändern (Ergänzungen unterstrichen):

				Profiling: automatisierte ~~jede Auswertung~~ Bewertung von ~~Daten oder~~ Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität Der generelle Einbezug von Datenauswertungen im Zusammenhang der Voraussage von Entwicklungen auch mit der wirtschaftlichen Lage ist aus Banksicht heikel.
DSG	4	3		**Kernanliegen: Keine Verschärfung der bewährten aktuellen Regelung** Gemäss Erläuterungsbericht soll die Regelung des Grundsatzes von Treu und Glauben gemäss Art. 4 VE-DSG materiell keine Änderungen gegenüber der aktuellen Fassung gemäss Art. 4 DSG enthalten (vgl. Erläuterungsbericht, S. 45 f.). Entgegen dieser Aussage wird nun aber in Abs. 3 der Grundsatz der «Erkennbarkeit» mit dem Zusatz «klarer» Erkennbarkeit verschärft. Der Hinweis auf terminologische Anpassung an die EU-DSGVO (vgl. Erläuterungsbericht, S. 46) ist schon deshalb verfehlt, weil die EU-DSGVO einem grundsätzlich anderen Grundkonzept als das Schweizer DSG folgt. Das Schweizerische DSG fusst auf dem bewährten Fundament der – aus dem Grundsatz von Treu und Glauben abgeleiteten – Erkennbarkeit der Datenbearbeitung im Rahmen einer klaren Zweckbindung. Ausnahmen stellen Persönlichkeitsverletzungen dar, ausser es werden überzeugende Rechtfertigungsgründe geltend gemacht, welche in einer Interessenabwägung obsiegen, und mittels angemessener Information der betroffenen Person mitgeteilt (vgl. Rosenthal/Jöhri, a.a.O., Art. 4 DSG N 2 ff.). Das zusätzliche Adjektiv «klar» macht die Regel keineswegs klarer, sondern im Gegenteil auslegungsbedürftiger und produziert damit gegenüber der bestehenden bewährten Fassung von Art. 4 Abs. 3 DSG unnötigerweise Rechts*un*sicherheit. Der Begriff «klar» ist deshalb ersatzlos zu streichen.
DSG	4	5		**Kernanliegen: Keine Verschärfung der bewährten aktuellen Regelung** Entgegen dem Erläuterungsbericht (S. 47) erfolgt nicht nur die Übernahme der bewährten Grundsätze gemäss bestehendem Art. 5 DSG. Vielmehr führt die gewählte Formulierung von Art. 4 Abs. 5 VE-DSG zu einer unnötigen **Verschärfung des Pflichtenhefts**. Die vorgeschlagenen Regeln sind überschiessend. Statt der Pflicht zur Überprüfung der Richtigkeit der Daten würde z.B. die Pflicht genügen, geeignete Massnahmen zu ergreifen, um die Richtigkeit der Daten sicherzustellen. Teilweise entstehen aus den überschiessenden Pflichten auch unnötige Rechts*un*sicherheit und Abgrenzungsprobleme zu anderweitigen bestehenden gesetzlichen Regeln. Beispielsweise wird ein allgemeiner Löschungsanspruch

				statuiert, welcher im Einzelfall mit anderweitigen gesetzlichen Dokumentations- und Aufbewahrungspflichten kollidieren kann. Die Formulierung von Art. 5 DSG ist wesentlich besser gelungen, weshalb diese Regelung als neue Formulierung von Art. 4 Abs. 5 VE-DSG zu übernehmen ist. Sollte wider Erwarten gleichwohl am neuen Vorschlag gemäss VE-DSG festgehalten werden, müsste zumindest der Satzteil «und wenn nötig nachgeführt wurde» gestrichen werden, da diese Aussage unklar und überflüssig ist. Zudem ist in den **Erläuterungen** klarzustellen, dass **keine Vernichtungspflicht** besteht, soweit gesetzliche oder regulatorische (aufsichtsrechtliche) Aufbewahrungspflichten dem entgegenstehen. Dies betrifft z.B. die Bestimmungen des Geldwäschereigesetzes, die eine Bank verpflichten, alle Informationen aufzubewahren, die mit der Information des Kunden oder mit aussergewöhnlichen Transaktionen zusammenhängen. Es gilt hier ganz grundsätzlich zu bedenken, dass eine Bank mit den hier angedachten auferlegten Pflichten im Tagesgeschäft rasch an ihre Grenzen stösst. Es ist einer Bank nur sehr schwer möglich, ein eingereichtes Ausweisdokument und die darauf verzeichneten Daten auf ihre Echtheit zu überprüfen.
DSG	4	6		**Kernanliegen: Keine Verschärfung durch strengere Formvorschriften** Wie unter Abs. 3 wurde auch unter Abs. 6 eine unnötige vermeintliche Präzisierung eingefügt, indem die ausdrückliche Einwilligung nicht nur nach angemessener Information freiwillig, sondern neu zusätzlich «eindeutig» sein soll. Diese Neuformulierung ist verunglückt, da sie entgegen der Absicht gemäss Erläuterungsbericht (S. 45 ff.) eine Verschärfung und damit verbunden Rechts*un*sicherheit beinhaltet. Unklar bleibt insbesondere, ob das im Massengeschäft und insbesondere beim elektronischen Auftritt unumgängliche Abstellen auf Allgemeine Geschäftsbedingungen (AGB) weiterhin zulässig sein soll. Diese Frage muss klar mit ja beantwortet werden. Im Erläuterungsbericht (S. 47) wird zu Unrecht gefordert, dass die betroffene Person nicht gänzlich untätig bleiben darf, damit von einer «Einwilligung» ausgegangen werden kann. Mit dieser Auslegung wird de facto eine Formvorschrift aufgestellt, welche zahlreiche aus dem modernen Geschäftsleben nicht mehr wegzudenkende und datenschutzrechtlich unproblematische Anwendungen, welchen z.B. Regelungen in AGB zugrunde liegen, künftig verunmöglichen würde. Richtigerweise ist auf den Zweck der Datenbearbeitung abzustellen (Art. 4 Abs. 3 DSG). Soweit dieser für die betroffene Person erkennbar ist, muss die Einwilligung formunabhängig erfolgen

				können. Die bestehende Fassung von Art. 4 Abs. 5 DSG ist klarer und in sich stimmiger formuliert. Demzufolge sollte diese Fassung auch in Art. 4 Abs. 6 VE-DSG übernommen werden. Im Eventualfall ist aus systematischen Gründen zumindest das Profiling aus der Regelung zu entfernen. Der Umgang mit Profiling ist anderweitig im VE-DSG bereits detailliert geregelt (bzw. gemäss nachfolgenden Anträgen zu regeln), insb. in Art. 3 Bst. f. und in Art. 15 VE-DSG. Die zusätzliche Regelung auch in Art. 4 Abs. 6 VE-DSG produziert unnötige Doppelspurigkeiten mit der Folge von Abgrenzungsproblemen und Rechts*un*sicherheiten, und dies alles bei Themen, welche sogar unter Strafe gestellt sind (Art. 50 ff. VE-DSG).
DSG	5			**Kernanliegen: Informations- und Genehmigungspflichten setzen komplizierte sowie ressourcenintensive, interne Prozesse voraus und sind zu streichen, eventuell auf höchstens vier Wochen zu reduzieren**
DSG	5	1		Art. 5 Abs. 1 wiederholt lediglich einen anderweitig – u.a. in Art. 4 Abs. 1 VE-DSG – bereits statuierten Grundsatz und ist im Kontext von Art. 5 VE-DSG verwirrend, überflüssig und bietet der betroffenen Person keinen Mehrwert. Die konkrete anwendbare Regelung ergibt sich abschliessend aus den folgenden Absätzen von Art. 5 VE-DSG. Ein konkreter Anwendungsbereich von Abs. 1 ist nicht erkennbar, weshalb er ersatzlos zu streichen ist.
DSG	5	2 u. 3		Die Einschränkung, dass für eine Datenbekanntgabe ins Ausland eine **vorgängige Feststellung des Bundesrats** über die Angemessenheit des Datenschutzes im betreffenden Land notwendig ist, schränkt ungerechtfertigt und unnötig ein. Es ist durchaus denkbar, dass ein **Verantwortlicher gestützt auf eigene Abklärungen bzw. Kenntnisse** z.B. in Form einer «Legal Opinion» weiss, dass vor Ort ein angemessenes Datenschutzniveau gilt. Solche eigenen Abklärungen müssen zulässig sein. Umgekehrt kann dem Verantwortlichen nicht zugemutet werden, trotz Bedarf an Datenflüssen in ein bestimmtes Land darauf warten zu müssen, bis in unbestimmter Zukunft eine Einschätzung des Bundesrats vorliegt oder – mangels einer solchen – trotz besseren eigenen Kenntnissen bis zum Vorliegen der Einschätzung des Bundesrats immer die strengeren Voraussetzungen gemäss Abs. 3 einhalten zu müssen. Demzufolge ist Abs. 3 von Art. 5 VE-DSG wie folgt zu ergänzen (Ergänzungen unterstrichen):

				Liegt kein Entscheid des Bundesrats vor, dürfen Personendaten ins Ausland bekannt gegeben werden, wenn der Verantwortliche selbst festgestellt hat, dass ein angemessener Schutz gewährleistet ist oder wenn ein geeigneter Schutz gewährleistet ist durch: …
DSG	5	3 u. 5	3 c u. d	Die Regelung, wonach standardisierte Garantien und sog. «Binding Corporate Rules» (BCR) einer **Genehmigungspflicht von sechs Monaten** unterliegen, ist weder sachgerecht noch praktikabel (Art. 5 Abs. 3 Bst. c u. d i.V.m. Abs. 5 VE-DSG). Einerseits stellen standardisierte Garantien ebenso wie BCR blosse Unterkategorien der «spezifischen Garantien» i.S.v. Art. 5 Abs. 3 Bst. b VE-DSG dar und für letztere ist lediglich eine Informationspflicht vorgesehen (eine Genehmigung durch den EDÖB ist nicht erforderlich). Ferner ist eine Frist von sechs Monaten abzulehnen. Dasselbe gilt für die Möglichkeit des EDÖB, Informationen nachzuverlangen, was die sechsmonatige Frist erneuern würde. Eine solche Regelung würde jeden unternehmerischen Handlungsbedarf im Keim ersticken und typische Bankgeschäfte mit internationalem Konnex verhindern (vgl. unten zu Art. 6 Abs. 1 Bst. a u. b VE-DSG). Im Ergebnis würden die bewährten Instrumente standardisierte Garantien und BCR gar nicht mehr verwendet.
DSG	5	6		Die pauschale Informationspflicht bietet weder der betroffenen Person noch dem EDÖB einen Mehrwert. Dementsprechend kennt auch die EU-DSGVO keine entsprechende Informationspflicht. Art. 5 Abs. 6 VE-DSG ist deshalb ersatzlos zu streichen.
DSG	6			**Kernanliegen: Berücksichtigung der Bedürfnisse der Praxis bei Festlegung der Ausnahmetatbestände**
DSG	6	1	a	Die Anforderung, dass die betroffene Person «im Einzelfall» einwilligen muss, ist eine allzu strenge Einschränkung. Nach allgemeinen Grundregeln des Vertragsrechts genügt es, wenn die betroffene Person mit Bezug auf bestimmte wiederkehrende Sachverhalte generell gültig zustimmen kann, mithin nicht nur für einen aktuellen Einzelfall, sondern auch mit Wirkung für analoge künftige Fälle. Dies ist bereits heute unter geltendem DSG von Lehre und Praxis anerkannt. Andernfalls würde ein enormer unnötiger Aufwand generiert, welchen die betroffene Person selbst nicht mehr verstehen würde. Im Interesse einer immer mehr arbeitsteilig und international vernetzt organisierten Wirtschaft z.B. ist der Verzicht auf das Erfordernis der Einwilligung im Einzelfall zwingend nötig. Eine generelle Information, welche den betroffenen Personen den wiederkehrenden Sachverhalt und die damit verbundenen typischen Risiken

				erläutert, muss genügen. Viele Massengeschäfte mit notwendigerweise internationalem Konnex wären andernfalls gar nicht mehr durchführbar mit der Folge von starken Wettbewerbsverzerrungen zu Lasten von Schweizer Unternehmen und zum Nachteil schweizerischer Kunden (welchen in der Schweiz nur noch eine laufend eingeschränkte Produktepalette zu immer höheren Preisen zur Verfügung stünde). Gegen das Zustimmungserfordernis im Einzelfall sprechen auch die typischerweise engen zeitlichen Verhältnisse. Zu denken ist z.B. an Kauf und Verkauf von Effekten für Kunden im Ausland, Verwahrung von Effekten im Ausland, etc. Das Erfordernis der Zustimmung im Einzelfall würde auch die einschlägige Regulierung der FINMA torpedieren, welche das internationale Bankgeschäft und die damit notwendigerweise zusammenhängenden Informationsflüsse u.a. mit Blick auf die typischerweise knappen zeitlichen Verhältnisse gerade ermöglichen und sicherstellen will (vgl. Art. 42c FINMAG u. dazu FINMA-RS 2017/6 Direktübermittlung). Demzufolge ist die Einschränkung **«im Einzelfall» ersatzlos zu streichen**.
DSG	6	1	b	Art. 6 Abs. 1 Bst. b VE-DSG muss aus Gründen der Rechtssicherheit und Äquivalenz mit der Regelung der EU-DSGVO in Übereinstimmung gebracht werden. Demnach 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. Diese Präzisierung ist z.B. im Bankenbereich für zahlreiche Konstellationen nötig. Bei internationalen Transaktionen des Handels und der Verwahrung von Wertschriften z.B. tritt die Bank nach bewährter Praxis in eigenem Namen und bloss im Interesse der betroffenen Kunden auf. Andere Lösungen wären in Massengeschäften dieser Art gegenüber ausländischen Vertragspartnern der Bank nicht durchsetzbar und – selbst wenn – mit Blick auf den immensen Aufwand für den einzelnen Kunden extrem kontraproduktiv, weil der einzelne Kunde mit wesentlich höheren Gebühren konfrontiert wäre. Solche bewährten Strukturen liegen somit im klaren Interesse der betroffenen Kunden. Art. 6 Abs. 1 Bst. b ist daher wie folgt anzupassen (Ergänzungen unterstrichen): *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>;*
DSG	6	1	c Ziff. 2	Um schwierige Abgrenzungsfragen im Voraus auszuschliessen, sollten in Art. 6 Abs. 1 Bst. 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. Da es sich um ausländische Stellen und Verfahren handelt, dürfen deshalb nicht allein Schweizerische Traditionen massgebend sein. Vielmehr ist die Klausel offen zu formulieren, um auch wesentlich von Schweizer Traditionen abweichende Verfahrensformen zur Rechtsdurchsetzung zu erfassen (vgl. Werner Wyss, in: Nicolas Passadelis/David Rosenthal/Hanspeter Thür (Hrsg.), Handbücher für die Anwaltspraxis, Datenschutzrecht, Basel 2015, N 11.92 ff.). Demzufolge ist die Einschränkung «vor einem Gericht oder einer Verwaltungsbehörde» ersatzlos zu streichen. Art. 6 Abs. 1 Bst. c Ziff. 2 ist daher wie folgt anzupassen: *die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen ~~vor einem Gericht oder einer Verwaltungsbehörde~~;*
DSG	6	1	d	Vgl. Ausführungen zu Art. 6. Abs. 1 Bst. a VE-DSG. Anpassungsvorschlag: *die Bekanntgabe ~~im Einzelfall~~ notwendig ist, um das Leben oder die körperliche*
DSG	6	2		Art. 6 Abs. 2 VE-DSG ist **ersatzlos zu streichen**. Erstens ist eine Verpflichtung, den EDÖB trotz Ausnahmetatbestand zu informieren, unverhältnismässig. Typischerweise dürfte dies auch kontraproduktiv sein, da Ausnahmetatbestände i.d.R. zeitkritisch sind und keinen Aufschub dulden. Zweitens würde diese bereits (für Verantwortliche und Auftragsdatenbearbeiter) geltende Pflicht zu einer «*Meldeflut*» führen, welche der EDÖB gar nicht wird bewältigen können. Drittens würde der EDÖB über heikle Verfahren und (Geschäfts-) Geheimnisse informiert, ohne dass ein (sachlich gerechtfertigter) Grund dafür vorliegt und ohne Mehrwert für betroffene Personen. Zudem ist diese Pflicht dem EU Recht (inkl. ERK 108) fremd und somit ein kontraproduktiver Swiss Finish. Deshalb ist Abs. 2 ersatzlos zu streichen.
DSG	7	2		Art. 7 Abs. 2 VE-DSG führt Pflichten auf, welche gemäss Gesamtgefüge des VE-DSG ohnehin bereits bestehen. Diese Regelung ist demzufolge **ebenso wenig notwendig wie zusätzliche Präzisierungen in der Verordnung**. Letztere könnten **sogar kontraproduktiv** sein, da jedes Projekt eigene spezifische Datenschutzthemen generiert. Ein allgemeiner starrer Anforderungskatalog kann diesen Projekt-spezifi-

				schen Herausforderungen nicht gerecht werden. Vielmehr würde der Katalog Herausforderungen bestimmter Projekte gar nicht aufführen oder umgekehrt die Verantwortlichen zwingen, bestimmte Themen generell in jedem Projekt detailliert zu klären, obwohl diese je nach Projekt gar keine Rolle spielen. Allgemeine Präzisierungen würden somit einerseits per definitionem unvollständig bleiben und andererseits zu unnötigem Zusatzaufwand führen. Solche Detailregulierungen widersprechen sodann auch dem bewährten **prinzipienbasierten Ansatz** des DSG, an welchem der VE-DSG erklärtermassen festhalten will. Abs. 2 von Art. 7 VE-DSG ist demzufolge **ersatzlos zu streichen**. Soweit sich zu diesem Themenkreis wider Erwarten gleichwohl Präzisierungsbedarf ergeben sollte, ist der **Bundesrat** ohnehin generell – auch **ohne ausdrückliche spezifische Ermächtigung im Gesetz – befugt, die notwendigen Präzisierungen auf Verordnungsstufe zu erlassen**. Der Unterschied liegt darin, dass der Bundesrat gestützt auf eine ausdrückliche Anordnung, wie Art. 7 Abs. 2 VE-DSG sie vorsieht, zum Erlass von Verordnungsbestimmungen nicht nur berechtigt, sondern verpflichtet ist. Eine solche Notwendigkeit zum Erlass von Verordnungsbestimmungen besteht aber wie dargelegt aus heutiger Sicht nicht.
DSG	8 u. 9			Das vorgeschlagene **Konzept zur Erstellung von Empfehlungen der guten Praxis** ist im Kern zu begrüssen. Es lehnt sich an das bereits bestehende **Konzept von Selbstregulierungen der Branche** an, wie es sich z.B. im Bereich der Finanzwirtschaft bestens bewährt hat und von der Aufsichtsbehörde FINMA, dem EFD und den Schweizerischen Gerichten anerkannt ist (vgl. insbes. zahlreiche, äusserst hilfreiche Selbstregulierungen von SBVg und SFAMA). Der wesentliche Vorteil liegt darin, dass qua Selbstregulierung entweder **sehr knappe oder aber sehr komplexe gesetzliche Regelungen praxisnah und operativ umsetzbar präzisiert** werden können. Mit solchen Selbstregulierungen, neudeutsch auch «Codes of Conduct» genannt, werden **Mindeststandards** geschaffen, welche nach dem Prinzip «comply or explain» funktionieren. Datenschutzrechtlich gesprochen entspricht dies einer **«Safe Harbor»-Regelung**. Zur Erreichung dieses Ziels muss einerseits sichergestellt sein, dass die themenspezifischen Wünsche der Branche tatsächlich in die Regelung einfliessen. Andererseits muss die Regelung trotz grundsätzlich klärendem Ansatz einen ausreichenden Grad an **Prinzipienbasiertheit** aufweisen, damit jede betroffene Unternehmung **entsprechend individueller Grösse, Komplexität, Struktur und Risikoprofil ihres Geschäftsmodells eine angemessene Umsetzung** (so die bewährte Standardumschreibung der FINMA) des betreffenden Themas vornehmen kann.

				Diese Anforderungen sind durch spezifische Umformulierung von Art. 8 und 9 VE-DSG zu realisieren.
DSG	8			Der Wortlaut von Art. 8 VE-DSG lässt zu, dass der EDÖB Empfehlungen der guten Praxis mit einem Inhalt erlässt, welcher dem erklärten Willen der betroffenen Branchenvertreter widerspricht. Damit würde dieses Institut seinem Zweck nicht gerecht und würde sich ins Gegenteil verkehren (vgl. oben zu Art. 8 u. 9 VE-DSG). Richtigerweise muss (i) die **Initiative zum Erlass von Empfehlungen der guten Praxis zwingend von Branchenverbänden ausgehen**. (ii) Wenn die Vorschläge die einschlägigen **Datenschutzvorschriften einhalten, genehmigt der EDÖB** die Vorschläge in Form von Empfehlungen der guten Praxis. (iii) Führen die Verhandlungen zwischen Branchenvertreter und EDÖB nicht zu einer Regelung, welche dem von der Branche gewünschten Konzept entspricht, muss den **Branchenverbänden das Recht zustehen, die Vorschläge ohne Weiteres zurückzuziehen** und auf einschlägige Empfehlungen zu verzichten. (iv) Erlässt der EDÖB gleichwohl Empfehlungen der guten Praxis mit anderem Inhalt als von den Branchenverbänden gewünscht, muss dies in Form einer **von den Branchenverbänden anfechtbaren Verfügung** geschehen. (v) Der **EDÖB publiziert genehmigte Vorschläge der Branche** als Empfehlungen der guten Praxis. Art. 8 und 9 VE-DSG sind im vorstehenden Sinn umzuformulieren. Diese Lösung stellt auch die **Rechtstaatlichkeit der Regelung** sicher. Andernfalls stünde nämlich dem EDÖB eine kritische da allzu grosse Machtfülle zu, notfalls sogar gegen die Meinung der betroffenen Branchen Empfehlungen der guten Praxis zu erlassen. Entgegen etablierten rechtsstaatlichen und demokratischen Prinzipien würde er so de facto zum Gesetzgeber in Datenschutzthemen. Daraus ergäben sich auch zusätzliche Risiken einer nicht mehr in sich stimmigen Rechtsordnung. Im Extremfall könnte der EDÖB z.B. entgegen der Bankenbranche Empfehlungen der guten Praxis erlassen, welche etablierten von Bankaufsichtsgesetzgebung und FINMA-Praxis statuierten Regeln widersprächen. Damit wäre es den Banken verboten, die Empfehlungen des EDÖB einzuhalten, womit sich letztere ins Gegenteil verkehren würde: Statt einer erwünschten «Safe Harbor»-Regelung würde de facto eine Verbotsregelung geschaffen, indem es den Banken verunmöglicht würde, in einem bestimmten Bereich überhaupt tätig zu werden. Eine derartige Machtfülle darf dem EDÖB nicht von Gesetzes wegen zugestanden werden.

DSG	9	1		Art. 9 Abs. 1 VE-DSG geht sehr weit und stellt mit der gewählten Formulierung eine **unumstössliche Fiktion** auf. Mit Blick auf die Vielfalt des operativen Alltags sind innerhalb der von Empfehlungen der guten Praxis geregelten Materie aber Konstellationen denkbar, welche von den Empfehlungen nur unvollständig und unzureichend geregelt werden. Unter einer unumstösslichen Fiktion sind die erfassten Konstellationen eng auszulegen. Dies würde dazu führen, dass trotz Existenz von Empfehlungen zahlreiche Konstellationen vom «Safe Harbor» nicht profitieren. Damit verlören zahlreiche Empfehlungen ihren Wert. Stellen die Empfehlungen demgegenüber bloss eine Vermutung der Richtigkeit dar, besteht auslegungstechnisch mehr Spielraum, (zahlreiche) zusätzliche Konstellationen zu erfassen. Somit ist es zielführender, in Art. 9 Abs. 1 VE-DSG statt einer unumstösslichen Fiktion nur, aber immerhin die **Vermutung der Richtigkeit** zu statuieren. Diese Regelung wird auch der beabsichtigten Qualität der Empfehlungen als «Safe Harbor»-Regelung besser gerecht (vgl. oben zu Art. 8 u. 9 VE-DSG).
DSG	12			**Kernanliegen: Ersatzlose Streichung des ganzen Artikels** **Der Schutz und die Rechte verstorbener Personen gehören ins ZGB.** 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 anderen 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 anderen Erben das Bankkundengeheimnis uneingeschränkt gilt. Art. 12 VE-DSG ist auch unklar abgegrenzt zur im Rahmen der pendenten Erbrechtsreform geplanten Regelung des Auskunftsrechts von Erben nach neuem Art. 601a nZGB. Nach alldem ist Art. 12 VE-DSG jedenfalls geeignet, statt der – heute nach Erbrecht bereits bestehenden – Rechtssicherheit eher **Widersprüche zu bereits bestehenden gesetzlichen Regelungen** zu produzieren. Nicht berücksichtigt sind ausserdem die Rechte und Pflichten des Datenverantwortlichen (zum Beispiel Forderung auf Datenvernichtung im Zusammenhang mit der Weiterführung einer Hypothek, Aktenaufbewahrung etc.). 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. Sollte dieser ersatzlosen Streichung wider Erwarten nicht gefolgt werden, müsste in der Regelung von Art. 12 Abs. 1 Bst. a zumindest der Begriff «kostenlos» ersatzlos gestrichen werden.
DSG	13			**Kernanliegen: Reduktion der Informationspflichten auf das Wesentliche. Die Information über die Beschaffung von Personendaten muss auch in allgemeiner Form möglich sein. Die Informationspflichten sind zusätzlich zu präzisieren.**
DSG	13	1		Sinnvollerweise wird die Informationspflicht ausdrücklich auf **besonders schützenswerte Daten** und überdies auf **Datenbearbeitungen ausserhalb des (objektivierten) Erkennbarkeitshorizonts** i.S.v. Art. 4 DSG der betroffenen Person eingeschränkt. Dies folgt aus dem naheliegenden Grundsatz, dass alle anderen Daten entsprechend den Grundsätzen von Art. 4 VE-DSG für die betroffene Person erkennbar sind und demzufolge keiner (zusätzlichen) Information bedürfen.

				Klarzustellen im Gesetz ist, dass die Information sich jedenfalls auf den Zeitpunkt der Datenbeschaffung bezieht und sich auch die Richtigkeit und Vollständigkeit der Daten an diesem Zeitpunkt misst. Für spätere Änderungen kann keine Informationspflicht bestehen. Zudem hat Art. 13 VE-DSG aus Klarheitsgründen in sich konsequent dieselbe Terminologie zu verwenden. Es muss z.B. konsequent von «Dritten» gesprochen werden (wie in Abs. 1) und nicht von «Empfängern» (wie in Abs. 3 u. 4) und statt von «Identität» vom «Namen» des Verantwortlichen. Sofern eine Pflicht zur Beschaffung von Informationen im Gesetz angelegt ist, ist der Betroffene nicht noch separat zu informieren. Der Artikel sollte folglich dahingehend präzisiert werden, da insbesondere im Geldwäschereigesetz für Banken bereits Datenbeschaffungspflichten bestehen.
DSG	13	3		Die Informationspflicht wird auf **alle Personendaten** ausgeweitet, was zu erheblichem **Mehraufwand** für die Unternehmen führen wird. In den Erläuterungen sollte präzisiert werden, dass bei allfälligen Änderungen keine Nachinformation erfolgen muss. Art. 13 Abs. 3 VE-DSG verwendet die Begriffe «Dritter» und «Empfängerinnen und Empfänger», ohne diese genau zu definieren. Wir fordern deshalb, die Schlüsselbegriffe zu definieren, idealerweise in Form eines Glossars am Anfang des Gesetzes oder als Anhang, um die Begriffe entlang des ganzen Gesetzes durchgängig gleichförmig zu verwenden. Der gesamte Absatz ist unklar formuliert, was insbesondere die Abgrenzung der Pflichten des Verantwortlichen und des Auftragsdatenbearbeiters betrifft. Abs. 3 sollte deshalb **ersatzlos gestrichen** werden.
DSG	13	4		Die **Mitteilung der Identität und Kontaktdaten sämtlicher Auftragsdatenbearbeiter ist überschiessend** und weder sinnvoll noch nötig. Solche Pflichten kennt auch die **EU-DSGVO nicht**. Diese Anforderung ist somit kontraproduktiver **Swiss Finish**, der für die notwendige Äquivalenz nicht notwendig ist. Wenn schon, dann wäre von «Name» statt «Identität» zu sprechen. Zahlreiche Auftragsdatenbearbeiter sind zudem bloss für untergeordnete Tätigkeiten mandatiert. Die Offenlegung sämtlicher Auftragsdatenbearbeiter widerspricht deshalb auch dem datenschutzrechtlichen Verhältnismässigkeitsprinzip («need to know»). Auch gesetzliche Pflichten des Verantwortlichen müssen selbstverständlich widerspruchsfrei in das übrige datenschutzrechtliche Gesamtkonzept des Gesetzes, wozu u.a. Art. 18 Abs. 2 VE-DSG («need to know») gehört, eingebettet sein.

				Überdies greift die Offenlegung von Identität und Kontaktdaten sämtlicher Auftragsdatenbearbeiter massiv in berechtigte eigene Datenschutzinteressen und überdies in Geschäftsgeheimnisse des Unternehmens ein, welche gesetzlich geschützt sind (Art. 162 StGB). Es steht dem VE-DSG nicht an, in anderen Gesetzen geregelte Geheimnispflichten einfach zu missachten. Schliesslich würde die Liste sämtlicher Auftragsdatenbearbeiter kaum einen informativen Mehrwert produzieren. Zumindest innerhalb derselben Branche würde sich vermutlich zeigen, dass sehr viele Marktteilnehmer zur Unterstützung auf dieselben Auftragsdatenbearbeiter abstellen. Damit würde den betroffenen Personen de facto auch jedes Wahlrecht genommen, je nach Inhalt der Liste z.B. die Bank zu wechseln. Aufgrund all dieser Argumente kommt der Offenlegung von Identität und Kontaktdaten unter keinem vernünftigen Titel, nicht einmal unter den datenschutzrechtlichen Gründen i.e.S., ein sinnvoller Zweck zu. Im Gegenteil würde eine solche Offenlegung zur Verletzung berechtigter Datenschutzbedürfnisse des Unternehmens führen. Dies alles muss dazu führen, dass diese unnötigen Zusatzanforderungen **ersatzlos gestrichen werden**.
DSG	13	5		Diese Pflicht zur Weitergabe von Informationen **sprengt den Rahmen von Datenschutz i.e.S.** Die Regel fordert maximale Transparenz zum Preis eines hohen, unverhältnismässigen Aufwands. Da die Bestimmung die Datenbeschaffung durch Dritte regeln will, sind die relevanten Eckpfeiler wie insbesondere «erstmalige Speicherung» regelmässig gar nicht bekannt. Der dafür eingesetzte Dritte kennt diese Modalitäten naturgemäss viel besser. Wird der Verantwortliche direkt verpflichtet, müsste er deshalb aus Gründen seiner Sorgfaltspflicht immer zuerst den Dritten anfragen, bevor er gestützt auf dessen Angaben die betroffenen Personen informieren könnte. Dies ist im operativen Alltag weder sinnvoll noch zielführend. Solche direkten Informationspflichten sind aber auch gar nicht nötig. Wenn überhaupt, dann wäre eher zu überlegen, inwiefern eine Verpflichtung des Dritten zur indirekten Weitergabe implementiert werden soll. Dies wäre nach dem Gesagten jedenfalls sachlich näherliegend und wesentlich einfacher bzw. weniger aufwendig. Auch mit dieser Umsetzung bliebe die Regel aber infolge ihres schlechten Aufwand/Ertrags-Verhältnisses mehr als fraglich. Im Gesamtgefüge des VE-DSG muss eine allgemeine vorgängige Information an die betroffenen Kunden genügen, wonach bestimmte Daten zu bestimmten Zwecken an bestimme Kategorien von Dritten

				beschafft und gegebenenfalls auch bearbeitet werden (vgl. Art. 13 Abs. 1-3 VE-DSG). Der Abs. 5 bringt dazu keinen Mehrwert, sondern nur unnötigen Mehraufwand. Dieser Absatz ist deshalb **ersatzlos zu streichen**.
DSG	14	1		Der Bankkunde erteilt bereits durch das Anvertrauen der Gelder oder der Beanspruchung eines Kredites seine stillschweigende Zustimmung zur Datenbeschaffung. Eine explizite Informationspflicht ist im Bankwesen daher nicht notwendig. Art. 14 VE-DSG sollte eine solche Ausnahme daher vorsehen und wäre wie folgt zu ergänzen (Ergänzungen unterstrichen): *Die Informationspflicht nach Artikel 13 entfällt, wenn die betroffene Person ihre stillschweigende Zustimmung zur Datenbeschaffung- ~~etwa im Rahmen eines Bankgeschäftes~~ erteilt hat.*
DSG	14	4	a	Wir schlagen vor, die Bestimmung wie folgt zu formulieren (siehe hierzu die Ausführungen in Art. 21 VE-DSG): *a) wenn es sich beim Verantwortlichen um eine private Person handelt, falls überwiegende Interessen des Verantwortlichen dies erfordern ~~und er die Personendaten nicht Dritten bekannt gibt;~~*
DSG	14	6 (neu)		In der EU-DSGVO ist eine Bestimmung eingefügt, welche offenkundig unbegründete oder exzessive Anträge regelt. Der Schweizer Gesetzgeber muss eine vergleichbare Regelung aufnehmen. Nur so können «gleich lange Spiesse» erzielt und den wichtigen Anliegen der Verhinderung unnötigen Aufwands Rechnung getragen werden. Wir schlagen vor, den folgenden neuen Absatz zu ergänzen: *a) Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person, kann der Verantwortliche entweder ein angemessenes Entgelt verlangen, bei dem die Kosten für den Aufwand von Unterrichtung, die Mitteilung oder Durchführung der beantragten Massnahme berücksichtigt werden, oder* *b) sich weigern, aufgrund des Antrags tätig zu werden.*
DSG	15			**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 unabdingbar geworden sind. Zudem wirken sie sich auch positiv bei den Kunden aus, z.B. durch attraktive Preisgestaltung.
DSG	15	2		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 als **wettbewerbs- und innovationshemmend** 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 (Art. 15 Abs. 1 VE-DSG). Unabhängig davon gewissermassen «auf Vorrat» zu informieren produziert demnach keine zusätzliche Transparenz, sondern generiert lediglich unnötigen zusätzlichen Administrativaufwand. Weder die ERK 108 noch die EU-DSGVO sehen ein entsprechendes Äusserungsrecht vor. Die Regelung von Art. 15 Abs. 2 VE-DSG ist demzufolge ein kontraproduktiver und im Hinblick auf die Äquivalenz unnötiger Swiss Finish. **Automatisierte Entscheide** bringen gegenüber manuellen Entscheidungsprozessen auch 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. Es ist ausserdem auch nach Konsultation der Botschaft weitgehend unklar, wann genau eine automatisierte Einzelentscheidung vorliegt. Die Kunden können 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. Der Kunde wird darüber gemäss Art. 15 Abs. 1 VE-DSG bereits ausreichend informiert (z.B. mit einem Piktogramm). Eine Regel wie sie in Art. 15 Abs. 2 VE-DSG vorgeschlagen wird, würde daher den Kunden und Konsumenten unnötigerweise bevormunden. Zudem gehört die Information darüber, wie bestimmte Entscheide zustande kommen, zum Geschäftsgeheimnis eines Unternehmens, und 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 eine wichtige, differenzierende Kompetenz 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 die Innovationskraft der Wirtschaft erheblich beeinträchtigen, da der dafür eingesetzte Aufwand nicht angemessen geschützt werden könnte. Die Ausnahmebestimmung von Art. 21 Abs. 1 VE-DSG dürfte daher mehr die Regel als die Ausnahme bilden. Schliesslich ist die Befürchtung nicht von der Hand zu weisen, dass die Einführung einer Pflicht zur «Äusserung» in der Praxis zu einer **Begründungspflicht** führt und letztlich die Vertragsfreiheit eines Unternehmens erheblich einschränkt. 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 sehr unterschiedlich sein. Daraus ergibt sich, dass eine generelle Regelung für die gesamte Wirtschaft jedenfalls über das Ziel hinausschiesst. Nicht grundsätzlich abwegig ist es demgegenüber, soweit nötig für einzelne branchenspezifische Datennutzungen in einschlägigen Spezialgesetzen eine angemessene Regelung zu treffen, welche den Besonderheiten der betreffenden Branche gebührend Rechnung trägt. Aufgrund all dieser Argumente fordern wir dezidiert die **ersatzlose Streichung der Äusserungsrechts von Art. 15 Abs. 2 VE-DSG**.
DSG	15 u. 20			**Folgen** der ersatzlosen Streichung des Äusserungsrechts in Art. 15 Abs. 2 VE-DSG: Folgerichtig ist **auch der entsprechende thematische Abschnitt in Art. 20 Abs. 3 VE-DSG ebenfalls zu streichen**. 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 EU-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.

DSG	16			Die Regelung der Datenschutz-Folgenabschätzung (DSFA) im Vorentwurf erachten wir im Grundsatz als überflüssig. Die Forderung von Art. 8bis der revidierten ERK 108, bei geplanten Datenbearbeitung die Risiken einzuschätzen, wird durch Art. 11 VE-DSG (Datensicherheit) bereits erfüllt. Wir erachten diese Regelung im vorliegenden Kontext für verzichtbar, zumal die Folgeabschätzungen stark interpretationsbedürftig bleiben und zu einem grossen, nicht absehbaren Aufwand führen, ohne dass ein Datenschutzmissbrauch letztlich verhindert werden könnte. Wir fordern daher ihre **Streichung**. Sofern an einer eigenen gesetzlichen Regelung der DSFA festgehalten wird, ist folgendes zwingend zu beachten. Die Pflicht, eine Datenschutz-Folgenabschätzung durchzuführen, ist im vorliegenden VE-DSG viel zu weit gefasst. Der Natur der Sache nach muss sich die Regelung **auf hohe Risiken beschränken**, wobei die Erheblichkeit – entsprechend der Regelung gemäss EU-DSGVO – aufgrund des gemäss DSFA erreichten Endresultats zu beurteilen ist. Mithin liegen erhebliche Risiken nur vor, soweit **selbst nach Implementierung geeigneter Massnahmen** weiterhin hohe Risiken verbleiben. Im aktuellen Entwurf würde die Regel ohne Notwendigkeit enormen Aufwand produzieren, welcher überdies sogar einen klaren, für die Äquivalenz unnötigen **Swiss Finish** darstellen würde. Überdies bestehen zahlreiche Spezialregeln, welche bestimmte Datenflüsse bereits einer anderweitigen Überwachung unterstellen. Im Bankenbereich wird z.B. der notwendige niederschwellige Datenfluss an ausländische Stellen (welche nicht Behörden sein müssen) gemäss Art. 42c FINMAG durch die FINMA überwacht (vgl. neues FINMA-RS 2017/6 «Direktübermittlung»). Solche «doppelten» Überwachungen sind aus Effizienzgründen und zur Vermeidung von Widersprüchen zu vermeiden. Wie dieses Beispiel zeigt würde eine zusätzliche Überwachung durch den EDÖB dem Zweck der Regelung von Art. 42c FINMAG und des einschlägigen FINMA-RS 2017/6 offensichtlich zuwiderlaufen, im Interesse von teilweise sehr kurzen Fristen für notwendige Datenflüsse klare und rechtssichere Regeln für eine rasche Lösung der Thematik im Einzelfall zur Verfügung zu stellen. Andernfalls wären Banken international von zahlreichen wichtigen Geschäftssparten faktisch ausgeschlossen. Sofern an einer Regelung festgehalten wird, wäre Art. 16 VE-DSG aus den genannten Gründen wie folgt neu zu fassen (Ergänzungen unterstrichen, vgl. dazu im **Einzelnen die nachfolgenden Begründungen unten**):

				[1] Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen~~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.*
DSG	16	1		Der Ausdruck «erhöhtes Risiko» in Abs. 1 ist zu unbestimmt. Er geht zudem über die europäischen Vorgaben hinaus: **Art. 35 f. EU-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 angemessener Mehrwert gegenübersteht.
DSG	16	2		**Es ist zudem falsch, von einem Risiko für «die Grundrechte» der betroffenen Personen zu sprechen.** Das entspricht zwar mehr oder weniger der Regelung der EU-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 (vgl. oben).
DSG	16	3		**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. Denn auch dieser sehr grosse, nicht absehbare Aufwand könnte letztlich einen Datenmissbrauch nicht verhindern. - Selbst das europäische Recht verlangt nicht, die Aufsichtsbehörden von jeder Datenschutz-Folgenabschätzung zu informieren. Art. 36 Abs. 1 EU-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 EU-DSGVO ist zwar unklar formuliert, doch ergibt sich dies eindeutig aus den Erwägungsgründen der EU-DSGVO.
DSG	16	4		**Auch die Reaktionszeit des EDÖB von drei Monaten ist viel zu lang**. 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.
DSG	17			Diese Pflicht wird ohne **gezielte Eingrenzung in qualitativer und quantitativer Weise** uferlos. Entsprechend würden die Verantwortlichen, um dem Vorwurf einer strafbaren Handlung zu entgehen (vgl.

				Art. 50 Abs. 2 Bst. e VE-DSG), jeden noch so geringfügigen Verstoss melden. Der Beauftragte wäre ausser Stande, innerhalb dieser Papierflut wirklich wichtige Meldungen zeitgerecht zu erkennen und geeignete Massnahmen einzuleiten. In solchen Fällen sähe er sich selbst mit dem Vorwurf konfrontiert, trotz erhaltener Meldung nicht gehandelt zu haben. Insgesamt verkäme das Institut zum reinen Formalismus, welcher allerdings für alle Beteiligten äussert aufwendig wäre. Die Regelung krankt überdies am Ansatz, dass der Verantwortliche sich mit Erfüllung der Meldepflicht in Bezug auf die Verfehlungen, welche zur Datenschutzverletzung geführt haben, de facto gleich selbst anzeigen muss. Damit wird das strafrechtliche Grundprinzip, dass niemand sich selbst anzeigen muss (nemo tenetur), verletzt. Befolgt er die Meldepflicht nicht, wird er gleichwohl durch Nichteinhaltung derselben strafbar (Art. 50 Abs. 2 Bst. e VE-DSG). Umso schlimmer ist diese Regelung, wenn man davon ausgeht, dass seriöse Datenbearbeiter der Meldepflicht wohl nachkommen werden und gestützt darauf «als Dank» für ihre Versäumnisse sanktioniert werden. Demgegenüber werden die wirklich «schwarzen Schafe» die Meldepflicht nicht ausüben und – in vielen Fällen zu Recht – darauf vertrauen, dass der Skandal nicht erkannt wird und «unter dem Deckel» gehalten werden kann. Mit solchen Regelungen werden mithin schlicht die falschen Anreize gesetzt. Dies ist selbstredend zu verhindern. Das Dilemma könnte dadurch gelöst werden, dass der VE-DSG dem die Meldepflicht ausübenden Verantwortlichen einen «Bonus» oder gar Straffreiheit in Aussicht stellt, wie dies z.B. auch gemäss Kartellgesetz (KG) der Fall ist. Dies spricht übrigens auch dafür, dass – ebenfalls analog zum KG – die Sanktionskompetenz der Verwaltungsbehörde unter VE-DSG dem EDÖB zustehen soll und nicht den Strafbehörden und -gerichten (vgl. unten zu Art. 50 ff. VE-DSG). Ohnehin muss die aus einer allzu weit gefassten Papierflut resultierende kontraproduktive Papierflut eingedämmt werden. Dies geschieht am besten dadurch, dass – **wie dies die EU-DSGVO vorsieht** – **in qualitativer Hinsicht** nur **grobe Datenschutzverstösse** zu melden sind. Letztlich muss es um solche Fälle gehen, in welchen der Verantwortliche wegen der Dimension der Datenschutzverletzung nicht mehr aus eigener Kraft in der Lage ist, sämtliche geeignete Massnahmen einzuleiten und deshalb zur zielgerichteten Unterstützung an den EDÖB gelangt. Das qualitative Element der groben Datenschutzverletzung ist sodann mit einem **quantitativen Element** zu konkretisieren, wonach z.B. nur Fälle, in welchen Daten von **mindestens 100’000 Personen betroffen** sind, eine Meldepflicht auslösen.

				In zeitlicher Hinsicht ist sodann eine unverzügliche Meldung, wie sie Art. 17 Abs. 1 VE-DSG vorsieht, **nicht zielführend**. Massgebend muss der Zeitpunkt sein, in welchem dem Verantwortlichen **hinreichende Informationen** zur Beurteilung vorliegen, ob überhaupt eine Datenschutzverletzung stattgefunden hat und gegebenenfalls, ob sie eine meldepflichtige Dimension aufweist. Erst solche Klarheit über den Sachverhalt kann eine Meldepflicht auslösen. Es müssen mithin analoge Grundsätze zur Anwendung kommen, wie sie im Zivilrecht z.B. für die Beurteilung massgebend sind, ob eine Verjährungs- oder Verwirkungsfrist zu laufen beginnt. Erst eine mit solchen qualitativen, quantitativen und zeitlichen Einschränkungen versehene Meldepflicht für (grobe) Datenschutzverstösse ist zielführend und macht Sinn. Mit Blick auf den bereits stark reglementierten und beaufsichtigten Finanzbereich geben wir schliesslich zu bedenken, dass weitere Meldepflichten zu erheblichen Kompetenzproblemen zwischen Behörden führen können. In diesem Fall ist zu erwägen, ob Meldungen an den EDÖB nicht notwendig sein sollten, wenn der Datenschutzverantwortliche einer anderen Bundesaufsicht untersteht und allfällige Meldungen (beispielsweise aufgrund einer Verletzung eines Bankkundengeheimnisses) an diese zu richten hat (im Beispiel an die FINMA).
DSG	18			Mit dieser Bestimmung werden allgemeine Grundprinzipen des Datenschutzes wie z.B. im Abs. 2 der Grundsatz «need to know» kodifiziert. Aus Gründen der besseren Systematik und Übersichtlichkeit sollten diese in Art. 11 VE-DSG integriert und hier gestrichen werden.
DSG	19			Der VE-DSG weist bereits zahlreiche Informations- und Dokumentationspflichten auf. Durch Wiederholung in verändertem Wortlaut wie z.B. in Art. 19 VE-DSG entstehen bloss kontraproduktive Auslegungs- und Abgrenzungsprobleme, welche die notwendige Rechtssicherheit beeinträchtigen. Aus nachstehenden Ausführungen zu Bst. a und b von Art. 19 VE-DSG ergibt sich, dass diese Bestimmung hier zu streichen ist und der Inhalt, soweit notwendig, in andere Bestimmungen des VE-DSG integriert wird.
DSG	19		a	In Würdigung vorstehender Erwägungen und aus Gründen der notwendigen **Äquivalenz mit der EU-DSGVO** fordern wir, die in Bst. a von Art. 19 VE-DSG geregelte allgemeine Dokumentationspflicht durch die griffigere Anforderung zu ersetzen, dass ein **«Verzeichnis» als Dokumentation der Datenbearbeitungen** zu erstellen ist. Erst damit erhält die Bestimmung Art. 19 Bst. a VE-DSG eine gegen-

				über den zahlreichen anderweitig gemäss VE-DSG bestehenden Dokumentationspflichten klar fassbare, eigenständige Bedeutung. Aus Gründen der leichteren Auffindbarkeit und im Interesse der besseren Verständlichkeit des VE-DSG ist die im vorstehenden Sinn präzisierte Regelung von Art. 19 Bst. a VE-DSG systematisch **besser bei Art. 11 VE-DSG zu integrieren**. Wir geben zudem zu bedenken, dass die Dokumentation jeder Datenbearbeitung in einer Unternehmung einen grossen Aufwand verursachen und abschliessend (bei Strafandrohung) gar nicht möglich sein dürfte. So bearbeitet bspw. eine Bank täglich tausende von Daten ihrer Kunden, die personenbezogen sind. Diesem Umstand muss besser Rechnung getragen werden.
DSG	19		b	Diese Pflicht geht sehr weit, ohne dass ein klarer datenschutzrechtlicher Mehrwert erkennbar ist. Selbst die EU-DSGVO kennt solche Pflichten nicht. Nur schon aus Gründen der notwendigen **Äquivalenz** sollte deshalb darauf verzichtet werden. Kommt dazu, dass weder der Verantwortliche noch dessen Auftragsdatenbearbeiter selbst umfassend beurteilen können, welche Daten für welche Empfänger überhaupt (noch) von Interesse sind. Nur mit Bezug auf solche Daten würde sich aber eine Information überhaupt rechtfertigen. Die betroffene Person selbst kann dies viel besser beurteilen als Verpflichteter und Auftragsdatenbearbeiter. Pauschale «Massen»-Informationen an alle möglichen Adressaten würden nur unnötigen Aufwand beim Abwesenden und Unklarheiten bei den zahlreichen Empfängern generieren und wären überdies **kontraproduktiv**, da gesetzlich normierter klarer Verstoss gegen das datenschutzrechtliche Prinzip der Verhältnismässigkeit (Grundsatz «need to know»). Dahingehende Ansprüche der betroffenen Personen bestehen bereits nach **Art. 25 VE-DSG** (vgl. insb. Abs. 1 Bst. c). Insbesondere erscheint es nicht praktikabel, wenn Kunden informiert werden müssten, nachdem die Geschäftsbeziehung längst beendet ist. Nach alledem bleibt es besser den betroffenen Personen überlassen, die aus eigener, besserer Wahrnehmung wichtigen und richtigen Ansprüche gestützt auf Art. 25 Abs. 1 Bst. c VE-DSG geltend zu machen. Art. 19 Bst. b VE-DSG verbessert diesen Schutz wie dargelegt nicht und ist am besten zu **streichen**. Schliesslich muss es möglich bleiben, während der Kundenbeziehung Daten zu vernichten, ohne den Kunden zu informieren, sowie auch Kundendaten jederzeit zu löschen bzw. zu vernichten, sofern diese nicht aufbewahrt werden müssen (bspw. Massendaten wie Kontoauszüge).

DSG	20 u. 21			**Kernanliegen: Einführung von Mechanismen zur Verhinderung des Missbrauchs des Auskunftsrechts**
DSG	20			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 aber 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.
DSG	20	1		Dem zunehmenden **Missbrauch des Auskunftsrechts** für datenschutzfremde Zwecke ist ein Riegel zu schieben. Die Vergangenheit hat leider gezeigt, dass einerseits datenschutzrechtliche Begründungen viel zu leicht vorgeschoben werden können, um eine kostenlose Beschaffung von Beweismitteln durchzusetzen. Andererseits hat die Anzahl querulatorischer, kosten- und ressourcenintensiver Fälle zu reinen Schikanezwecken ebenfalls stark zugenommen. Aus diesen Gründen ist der Ansatz falsch, das **Auskunftsrecht generell kostenlos** auszugestalten. Damit wird ein Grundprinzip verletzt, welches ansonsten in der Rechtsordnung generell gilt. Dementsprechend ordnet auch die EU-DSGVO keine allgemeine Kostenlosigkeit an (Art. 12 Ab. 5 EU-DSGVO). Die von Art. 20 Abs. 1 VE-DSG angeordnete pauschale Kostenlosigkeit der Auskunft ist deshalb **nicht äquivalent** und demzufolge ersatzlos zu streichen. Stattdessen ist 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, muss es doch 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 Bst. a EU-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 unten zu Art. 21 VE-DSG). Der **Missbrauch des Auskunftsrechts**, namentlich die **zweckentfremdete Nutzung zur Beweismittelausforschung,** ist heute an der Tagesordnung und belastet die Unternehmen. Da der Herausgabeanspruch nach VE-DSG neu auch während Gerichtsverfahren gelten soll, dürfte der Trend zu Missbräuchen noch weiter zunehmen. Deshalb ist das Auskunftsrecht so anzupassen, dass es für die (datenschutzfremde) Beweismittelausforschung nicht mehr interessant ist, z.B. indem der Auskunftspflichtige wählen kann, die Auskunft nicht mehr in Form einer Kopie an den Auskunftssuchenden zu erstatten, sondern an eine **dritte Stelle**, welche die Verletzung des Datenschutzes stellvertretend prüft oder wo die Unterlagen eingesehen, aber nicht mitgenommen werden können. Alternativ wäre auch möglich, dass die betroffene Person ihr Interesse bei der Auskunftsanfrage darlegen muss oder die Schwelle zur Annahme eines Missbrauchs des Anfragenden gesenkt wird. Schliesslich fordern wir zur Eindämmung des Missbrauchs und um die verfahrensrechtlichen Regeln gemäss den einschlägigen Verfahrensordnungen wie z.B. der ZPO nicht zu verwässern, die **Wiedereinführung der Regel von Art. 2 Abs. 2 Bst. c DSG** (Nichtanwendbarkeit des DSG auf hängige Zivilprozesse und andere Verfahren). Ohne diese Regelung stünde das neue DSG im Widerspruch zum austarierten System der Mitwirkungspflichten und Verweigerungsrechte der Zivil- und Strafprozessordnung (vgl. Art. 160 ff. ZPO und Art. 157 ff. StPO). Während eines hängigen Zivil- und Strafverfahrens darf kein Auskunftsrecht bestehen. Vgl. dazu schon vorne zu Art. 2 Abs. 3 VE-DSG.
DSG	20	2	a	Aus systematischen Gründen ist – wie bereits bei Art. 13 Abs. 2 Bst. a bzw. Abs. 4 VE-DSG erwähnt – statt von «Identität» besser von «Name» und Kontaktdaten des Verantwortlichen bzw. des Auftragsdatenbearbeiters zu sprechen.
DSG	20	2	b	Wir empfehlen entsprechend bewährtem Auskunftsmechanismus die Präzisierung, dass die Information nur die Kategorien der bearbeiteten Personendaten beinhaltet. Dies entspricht Art. 15 Bst. b EU-DSGVO. Darüber hinauszugehen hiesse, einen mit Blick auf das gesetzgeberische Ziel der Äquivalenz unnötigen und kontraproduktiven Swiss Finish zu setzen. Anpassungsvorschlag (Ergänzung unterstrichen):

				Die Kategorien der bearbeiteten Personendaten
DSG	20	2	e	Die geforderte Information über das Vorliegen einer automatischen Einzelfallentscheidung darf hier, im Rahmen der allgemeinen Auskunftspflicht, nicht eine detaillierte Auflistung aller in der Vergangenheit ausgeführten automatischen Einzelfallentscheidungen beinhalten. Vielmehr ist hier bloss ein allgemeiner Hinweis notwendig, in welchen Bereichen bzw. zu welchen Themen gegebenenfalls automatische Einzelfallentscheidungen erfolgen. Andernfalls ergäbe sich im Rahmen von Art. 20 eine unübersichtliche Vermischung des allgemeinen Auskunftsanspruchs mit individueller Information zu einem konkreten Fall. Letzteres hätte, wenn überhaupt, losgelöst vom allgemeinen Auskunftsrechts unter Art. 15 VE-DSG zu geschehen (vgl. nachstehend zu Art. 20 Abs. 3 VE-DSG u. oben zu Art. 15 u. 20 VE-DSG).
DSG	20	2	f	Wir erachten es als ausreichend, wenn die Herkunft der Personendaten dann angegeben werden muss, wenn die Daten nicht bei der betroffenen Person selbst erhoben wurden. Dies entspricht Art. 15 Abs. 1 Bst. g EU-DSGVO. Anpassungsvorschlag (Ergänzungen unterstrichen): *Die verfügbaren Informationen über die Herkunft der Personendaten**,** falls diese nicht bei der betroffenen Person erhoben wurden*
DSG	20	2	g	«Empfänger» der Daten schliesst auch Auftragsdatenbearbeiter ein. Es ist nicht praktikabel und kann operativ nicht sichergestellt werden, sämtliche Auftragsdatenbearbeiter inkl. Identität und Kontaktdaten zu nennen (vgl. auch EU-DSGVO, wonach in Art. 15.1.b nur die Angabe von Kategorien von Empfängern verlangt wird). Anpassungsvorschlag: *Gegebenenfalls die Informationen nach Art. 13 Abs. 2 Buchstabe d (neu) und Abs. 3 ~~und 4~~*.
DSG	20	3		Der von Art. 20 Abs. 3 Halbsatz 2 VE-DSG geforderte Umfang des Auskunftsrechts (Informationen über Ergebnis, Zustandekommen und Auswirkungen der Entscheidung) ist mit Blick auf die anderweitig im VE-DSG bereits bestehenden weitreichenden Informationspflichten weder sinnvoll noch nötig und produziert ohne Mehrwert (z.B. in Form von mehr Transparenz) lediglich einen **unnötigen zusätzlichen**

				Administrativaufwand. Eine derart weitgehende Begründungs- bzw. Rechtfertigungspflicht ist datenschutzrechtlich nicht zu rechtfertigen. Sie würde ausserdem zwangsläufig zu einer Offenlegung von Geschäftsgeheimnissen z.B. in Form von internen Entscheid- und Ablaufverfahren führen. Die Regelung würde auch zu Unrecht eine **Vermischung des allgemeinen Auskunftsrechts mit individuellen Auskünften zu Einzelfallentscheidungen** produzieren. Eine gestützt auf Art. 20 VE-DSG erteilte allgemeine Auskunft hat in allgemeiner, übersichtlicher und leicht verständlichen Form den Anforderungen an die Auskunftspflicht zu genügen. Solche allgemeinen Auskünfte dürfen deshalb nicht mit einer Auflistung sämtlicher in der Vergangenheit durchgeführten individuellen Entscheidungen wie z.B. automatisierten Einzelfallentscheidungen ergänzt werden. Dies würde den Rahmen einer vernünftigen Auskunftserteilung sprengen und wäre auch für den Adressaten nicht mehr leicht 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. Darüber hinaus ist aber ein vom allgemeinen Auskunftsrecht losgelöstes individuelles Auskunftsrecht mit Bezug auf Ergebnis, Zustandekommen und Auswirkungen jeder Entscheidung generell abzulehnen. Die Auskunftspflicht würde damit erheblich ausgeweitet, wäre entsprechend massiv aufwendiger als bisher, ohne dass damit ein besserer Schutz der betroffenen Personen erreicht würde. Sehr viele Entscheidungen liegen im Rahmen dessen, was für die betroffenen Personen ohne weiteres erkennbar ist (vgl. Art. 4 Abs. 3 VE-DSG). Soweit eine Informationspflicht vorgeschrieben ist, muss diese auch genügen. Gestützt auf eine **angemessene Information** kann jede Person eigenverantwortlich entscheiden, ob sie die vorgeschlagene Form der Entscheidung akzeptieren will oder nicht. Die vom VE-DSG vorgeschlagene Regelung geht sodann klar über den von den EU-Anforderungen gesetzten Rahmen hinaus (vgl. Art. 15 Abs. 1 Bst. h EU-DSGVO). Dies stellt einen mit Blick auf die Äquivalenz unnötigen und kontraproduktiven Swiss Finish dar, der abzulehnen ist. Zusammenfassend ist die Regelung von Art. 20 Abs. 3 VE-DSG 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 Einzelentscheide beschränken.
DSG	20	5		Vgl. die Ausführungen zu Art. 7 VE-DSG. Anpassungsvorschlag:

				Lässt der Verantwortliche Personendaten von einem Auftragsdatenbearbeiter bearbeiten, so bleibt er auskunftspflichtig. ~~Der Auftragsbearbeiter ist hingegen auskunftspflichtig, wenn er nicht bekannt gibt, wer der Verantwortliche ist, oder wenn dieser keinen Wohnsitz in der Schweiz hat.~~
DSG	20	6		Wir empfehlen, an dieser Stelle ausdrücklich zu erwähnen, dass es sich beim Auskunftsrecht um ein subjektives höchstpersönliches Recht handelt.
DSG	20^{bis} (neu)			Die Ausnahmetatbestände von Art. 21 VE-DSG sind zu eng formuliert und inkonsistent. Die müssen in nachfolgendem Sinn **präzisiert und erweitert werden**: So ist beispielsweise 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 Bst. a VE-DSG). Gleichwohl ist die Informationspflicht aber dann nicht nachzuholen, 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 EU-DSGVO vorsieht (Art. 12 Abs. 5 Bst. b EU-DSGVO). Dies gilt umso mehr, als das Auskunftsrecht neu bei jeder Datenbearbeitung greift. Insbesondere wird es keine Beschränkung mehr auf Datensammlungen geben. Nicht nachvollziehbar ist auch, weshalb die Informationspflicht nach gesetzlicher Vorschrift nur bei indirekter Beschaffung durch Dritte entfallen soll (Art. 14 Abs. 2 Bst. a VE-DSG). Umso mehr muss die Informationspflicht bei direkter Beschaffung entfallen. 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 u. Art. 20 Abs. 2 Satz 1 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 (Werner Wyss, a.a.O., N 11.46). 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. Ein Auskunftsbegehren erfasst sachlogisch immer nur Daten über die antragstellende betroffene Person selbst. Nicht herauszugeben sind deshalb sämtliche Daten, welche Drittpersonen betreffen. Andernfalls würden mit der Datenherausgabe datenschutzrechtliche Ansprüche Dritter verletzt. Können solche Daten über Dritte nicht von den Daten über die betroffene Person getrennt werden, sind erstere z.B. mittels Schwärzung unkenntlich zu machen. Der Auskunftsverpflichtete ist auch vor Auskunftsbegehren zu schützen, welchen klarer Rechtsmissbrauch zu Grunde liegt (vgl. bereits oben zu Art. 20 Abs. 1 VE-DSG). Typische Fallgruppen klar rechtsmissbräuchlicher Geltendmachung des Auskunftsrechts sind aus Gründen der Rechtssicherheit direkt im Gesetzestext aufzuführen, insbesondere die Geltendmachung des Auskunftsrechts ohne erkennbaren sachlichen Grund oder die exzessive Geltendmachung des Auskunftsrechts mit häufiger Wiederholung, welche sachlich nicht nachvollziehbar ist. Es existiert im Vorentwurf kein pauschales Recht, die Herausgabe der Kommunikation zwischen der Bank und einem extern mandatierten Anwalt zu verweigern. Wichtig ist in diesem Zusammenhang, dass das Unternehmen aus rechtsstaatlichen Gründen nicht verpflichtet werden darf, interne Abklärungen zur Risikolage und zu den Prozesschancen im Vorfeld eines Prozesses herausgeben zu müssen, gehören solche Abklärungen doch zum Geschäftsgeheimnis eines jeden Unternehmens. Dies betrifft im Bankbe-

				reich etwa die Korrespondenz zwischen Banken und Rechtsanwälten oder Steuer- und Unternehmensberatern. Mit dieser Ausnahmeregelung werden verpönte «fishing expeditions» verhindert. Dies ist rechtsstaatlich mit allen Mitteln zu fördern so auch im Datenschutzrecht. Unter dem Geschäftsgeheimnis verstehen wir Tatsachen, die weder offenkundig noch allgemein zugänglich sind. Die Bank muss sodann ein Interesse und den Willen haben, diese Tatsachen geheim zu halten. Zielführend ist es deshalb, direkt in einem neuen Art. 20bis VE-DSG aufzuführen, dass solche Daten der vorstehend skizzierten Art nicht herauszugeben sind. Auch in der EU-DSGVO finden sich solche Ausnahmen und Einschränkungen. Zusammenfassend handelt es sich insbesondere um nachfolgend aufgeführte Daten: Formulierungsvorschlag für Art. 20bis VE-DSG (neu): *Nicht der Herausgabepflicht unterstehen folgende Datenkategorien:* *a) 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.* *g) Unterlagen aus dem Verkehr des Verantwortlichen mit einem Anwalt oder einem anderen beauftragten Dienstleister wie etwa Steuer- oder Unternehmensberater.*
DSG	21			Unter dem Vorentwurf (Art. 21 Abs. 1 i. V. m. Art. 14 Abs. 4 Bst. a VE-DSG) wie auch dem geltenden Recht (Art. 9 Abs. 4 DSG) ist es beispielsweise nicht möglich, die Auskunft bei einem überwiegenden

				Interesse der Bank zu verweigern, wenn die Personendaten einem Dritten (z.B. FINMA oder mandatierter Rechtsanwalt) weitergegeben wurden. Die fehlende Datenweitergabe an Dritte darf nicht Voraussetzung für die Auskunftsverweigerung sein, sondern ist in Art. 14 Abs. 4 Bst. a VE-DSG zu streichen. Dies betrifft etwa Fälle von Streitigkeiten zwischen Bank und einem Kunden. Wenn in solchen Fällen die Bank einen externen Rechtsanwalt mandatiert ein Gutachten zu erstellen, muss sie dieses Gutachten allenfalls in einem späteren Zivilprozess publik machen, denn dabei wurden ja klarerweise Daten an Dritte weitergegeben.
DSG	21	3 (neu)		Mit Blick auf die oben dargelegten Risiken des Missbrauchs des Auskunftsrechts, namentlich die **zweckentfremdete Nutzung zur Beweismittelausforschung**, muss ein effektiver **Mechanismus gegen solchen Missbrauch** vorgesehen werden, welcher das Auskunftsrecht für die (datenschutzfremde) Beweismittelausforschung nicht mehr interessant macht. Wir empfehlen, eine in der Praxis bewährte Vorgehensweise aus dem Bereich der Strafverfolgung anzuwenden (vgl. Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI); SR 361): Demnach kann der Verantwortliche bei begründetem Verdacht auf Missbrauch die herauszugebenden Personendaten einem Dritten (bspw. dem EDÖB) übergeben. Dieser würde anstelle des Gesuchstellers die Einhaltung bzw. Verletzung des Datenschutzes prüfen und sein Prüfergebnis in Form einer anfechtbaren Verfügung vorlegen (vgl. analoge Regelung in Art. 8 Abs. 2 BPI). Formulierungsvorschlag für Art. 21 Abs. 3 (neu): *Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche* *a) entweder ein angemessenes Entgelt verlangen, bei dem die Aufwandkosten für den Aufwand von Unterrichtung, Mitteilung oder Durchführung der beantragten Massnahme berücksichtigt werden, oder* *b) sich weigern, aufgrund des Antrags tätig zu werden.* (Eine analoge Formulierung drängt sich überdies auch bei Art. 14 in einem neuen Abs. 6 auf, vgl. oben). Alternativ könnte eine Kostenregelung eingeführt werden, die sich bspw. am Rechtsschutzinteresse des Gesuchstellers orientiert. Falls datenschutzfremde Interessen überwiegen, könnte eine höhere Gebühr verlangt werden; im umgekehrten Fall wäre eine tiefere Gebühr angezeigt (vgl. zu den Kosten einer Auskunft ferner oben zu Art. 20 Abs. 1 VE-DSG).

DSG	23	1	d	Aufgrund der richtigen Neukonzeption ist nur das **elektronische Profiling gesamtheitlich in Art. 15 VE-DSG** zu regeln. Demzufolge ist hier Abs. 1 Bst. d von Art. 23 VE-DSG ersatzlos zu streichen (vgl. oben zu Art. 3 Bst. f. u. Art. 15 VE-DSG).
DSG	23	2	d	Die Relevanz von Profiling sollte wie in der EU-DSGVO auf automatisierte Einzelentscheidungen beschränkt werden. Zudem ist das elektronische Profiling gesamtheitlich in Art. 15 VE-DSG zu regeln. Wir beantragen die **ersatzlose Streichung dieses Swiss Finish.**
DSG	24	1		Die Rechtfertigung durch «Gesetz» ist weiter zu definieren; andernfalls besteht ein Ungleichgewicht zwischen datenschutzrechtlichen und sonstigen rechtlichen Pflichten, welche auf derselben Stufe stehen müssen. Anpassungsvorschlag (Ergänzungen unterstrichen): *Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse ~~oder durch Gesetz~~ gerechtfertigt ist <u>oder auf rechtlichen Pflichten beruht</u>.*
DSG	24	2		Der Begriff «möglicherweise» ist mangels Aussagekraft und Mehrwert unnötig, demzufolge in Gesetzestexten auch gänzlich unüblich und deshalb ersatzlos zu streichen.
DSG	24	2	a	Zur Herstellung eines in sich stimmigen Gesamtkonzepts ist hier dieselbe Ergänzung anzubringen («*oder einer Person, zu deren Gunsten oder in deren Interesse der Vertrag abgeschlossen wird*»), wie sie auch unter Art. 6 Abs. 1 Bst. b VE-DSG notwendig ist (vgl. zur Begründung im Einzelnen dort).
DSG	24	2	c	Die Einschränkung gemäss Art. 24 Abs. 2 Bst. c Ziff. 1 VE-DSG ist nicht sachgerecht und sollte gestrichen werden. Sie verkennt, dass bspw. Massnahmen der sozialen Hilfe (Art. 3 Bst. c Ziff. 6 VE-DSG) von zentraler Bedeutung für die Beurteilung der Kreditwürdigkeit sein können. Ein Verzicht darauf würde zu Fehlbewertungen führen, was nicht im Interesse der betroffenen Person sein kann.
DSG	24	2	g (neu)	Schliesslich ist mit Art. 24 Abs. 2 Bst. g (neu) VE-DSG ein Rechtfertigungsgrund zu ergänzen, welcher den Einsatz neuer Technologien (insbesondere Profiling) zur Steigerung der Sicherheit bzw. der Prävention von Straftaten gegen das Vermögen der betroffenen Person ermöglichen würde.

				Formulierungsvorschlag für Art. 24 Abs. 2 Bst. g VE-DSG (neu): *die Daten zur Erhöhung der Sicherheit und Vermeidung von erheblichen Nachteilen für die betroffene Person bearbeitet werden, wofür sie auch Profiling durchführen kann.*
DSG	25	1	c	Wie bereits oben im Zusammenhang mit Art. 4 Abs. 4 und 5 VE-DSG (Grundsätze) erwähnt, können zwingende gesetzliche Vorschriften oder gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter der Vernichtung oder Löschung von Personendaten entgegenstehen (vgl. obenstehende Ausführungen zu Art. 4 VE-DSG). Anpassungsvorschlag (Ergänzungen unterstrichen): *Personendaten berichtigt werden; ~~, gelöscht oder vernichtet werden~~.*
DSG	25	1	d (neu)	Vgl. die Ausführungen zu Art. 25 Abs. 1 Bst. c. Formulierungsvorschlag für Art. 25 Abs. 1 Bst. d VE-DSG (neu): *Personendaten gelöscht oder vernichtet werden, sofern zwingende gesetzliche Vorschriften oder gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter dem nicht entgegenstehen*
DSG	25	3		Vgl. Ausführungen zu Art. 25 Abs. 1 Bst. c. Anpassungsvorschlag (Ergänzungen unterstrichen): *Die klagende Partei kann zudem verlangen, dass die Vernichtung, sofern zwingende gesetzliche Vorschriften oder gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter dem nicht entgegenstehen, die Berichtigung, die Vernichtung, das Verbot der Bearbeitung, namentlich das Verbot der Bekanntgabe an Dritte, der Bestreitungsvermerk oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.*
DSG	38	1		Eine Amtszeitbeschränkung ist eine in der Schweiz unübliche Praxis mit fragwürdigem Nutzen. Wir beantragen die ersatzlose Streichung dieser Bestimmung.

DSG	39	1		Es wird beantragt, die Formulierung «*Mitglied (…) der Verwaltung*» durch «*Mitglied (…) des Verwaltungsrats*» zu ersetzen. Damit wird sichergestellt, dass unter Mitglied der Verwaltung nicht die Verwaltung als Institution, sondern das oberste Exekutivorgan einer Gesellschaft verstanden wird. Anpassungsvorschlag (Ergänzungen unterstrichen): *Die oder der Beauftragte darf keine zusätzliche Erwerbstätigkeit ausüben. Sie oder er darf auch kein Amt der Eidgenossenschaft oder eines Kantons bekleiden und nicht als Mitglied der Geschäftsleitung, ~~der Verwaltung~~ des Verwaltungsrats, der Aufsichtsstelle oder der Revisionsstelle eines Handelsunternehmens tätig werden*
DSG	40 ff.			Die Regeln über die Rechtsprechung sind entsprechend unseren Ausführungen zu Art. 50 ff. VE-DSG (Sanktionen) anzupassen. Die Kompetenzen des EDÖB sind auf die derzeitigen Kompetenzen gemäss geltendem DSG zu beschränken. Weitergehende Kompetenzen müssen die von uns unter Art. 50 ff. VE-DSG vorgeschlagenen zusätzlichen Verwaltungsbehörde übertragen werden.
DSG	41	1		Unabhängig vom von uns vorgeschlagenen Konzept der verwaltungsinternen Gewaltenteilung (vgl. unten zu Art. 50 ff. VE-DSG) gehen die vorgesehenen Eingriffsrechte des EDÖB viel zu weit. Es darf keine Überprüfung ohne konkreten Anlass bzw. vorsorgliche Massnahmen geben. Der generelle Entzug einer aufschiebenden Wirkung oder einer Löschungsanordnung muss Sache der Gerichte bleiben. Die Einschränkung des geltenden DSG, wonach der EDÖB nur dann eine Untersuchung von sich aus durchführen kann, wenn eine grössere Zahl von Personen betroffen ist, müsste in Art. 41 Abs. 1 VE-DSG wiederaufgenommen werden. Das Verfahren vor dem Beauftragten ist ein öffentlich-rechtliches und daher auch nicht geeignet und auch nicht dazu vorgesehen, um Ansprüche aus der Persönlichkeitsverletzung geltend zu machen. Dafür muss der zivilrechtliche Weg beschritten werden. Folglich ist es auch nicht sachgerecht, dass jede Datenschutzverletzung untersucht wird. Dies würde sowohl beim EDÖB als auch beim Untersuchten unnötig wertvolle Ressourcen binden. Im Sinne der Verhältnismässigkeit sollte daher eine Untersuchung nur in schweren Fällen stattfinden. Anpassungsvorschlag (Ergänzungen unterstrichen):

				Der Beauftragte kann von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person eröffnen, wenn Anzeichen bestehen, dass eine Datenbearbeitung ~~gegen die Datenschutzvorschriften verstossen~~ die Persönlichkeit einer grösseren Anzahl von Personen verletzen könnte (Systemfehler)
DSG	41	3		Im Unterschied zur EU-DSGVO räumt der VE-DSG dem Beauftragen umfangreiche Ermittlungs- und Eingriffsbefugnisse ein. Dieser Swiss Finish ist abzulehnen. Diese Zwangsmassnahmen führen ausserdem zu Kompetenzkonflikten, wenn gleichzeitig eine Strafuntersuchung stattfindet. Aus der Sicht der Verhältnismässigkeit sollte daher nur derjenige über Zwangsmittel verfügen, der das Strafverfahren führt. Im Übrigen unterscheidet sich die Untersuchung gemäss DSG genau darin von jener gemäss KG. Im Kartellrecht ist es die Verwaltungsbehörde, welche das «Strafverfahren» führt und die Sanktionen ausspricht. Im reinen Verwaltungsverfahren besteht aber für spezialgesetzliche Untersuchungsbefugnisse kein Raum. Es ist ferner nicht einzusehen, weshalb für das Verfahren beim EDÖB nicht einfach wie im Verwaltungsrecht üblich, das VwVG anwendbar sein soll, wie das in Art. 44 ohnehin vorgesehen ist. Zudem ist fraglich, ob die Bestimmung im Einklang mit strafrechtlichen, untersuchungsrechtlichen und staatsrechtlichen Grundsätzen steht. Insbesondere ist unklar, wie vorzugehen ist, wenn ein gesetzliches/regulatorisches Mitwirkungsverweigerungsrecht und/oder Recht auf Aussageverweigerung besteht. Bei der Inspizierung von Räumlichkeiten müssten dieselben Voraussetzungen eingehalten werden, wie dies heute bei Hausdurchsuchungen der Fall ist. Anpassungsvorschlag (Ergänzungen unterstrichen): *Kommt das Bundesorgan oder die private Person der Mitwirkungspflicht nicht nach und hat der Beauftragte trotz angesetzter angemessener Frist die notwendigen ~~vergeblich versucht,~~ Auskünfte und Unterlagen nicht erhalten ~~einzuholen~~, so kann der Beauftragte im Rahmen einer Untersuchung, nach Erlass einer entsprechenden anfechtbaren Verfügung:* *a. ~~ohne Vorankündigung~~ Räumlichkeiten inspizieren;*
DSG	41	4		Diese Regelung ist zu präzisieren, zumal nicht klar ist, welche Überprüfungsbefugnisse der Beauftragte ausserhalb einer Untersuchung haben wird.

DSG	41	5		Wir regen an, in Art. 41 Abs. 5 VE-DSG auch den Interessen der angezeigten Person Rechnung zu tragen. Insbesondere soll die angezeigte Person vom Beauftragten über das weitere Vorgehen und das Ergebnis einer allfälligen Untersuchung informiert werden. Anpassungsvorschlag (Ergänzungen unterstrichen): *Wenn die betroffene Person Anzeige erstattet hat, informiert der Beauftragte sie über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung. Der Beauftragte hat dabei die Interessen der angezeigten Person zu berücksichtigen. Zudem hat der Beauftragte auch die angezeigte Person über sein weiteres Vorgehen und das Ergebnis einer allfälligen Untersuchung zu informieren.*
DSG	42			Diese Bestimmung ist **ersatzlos zu streichen**. Die geltende Regelung, wonach der EDÖB beim Bundesverwaltungsgericht eine entsprechende Massnahme beantragen muss, hat sich bewährt und sollte nicht ohne Not geändert werden. Auch hier besteht kein Erfordernis über die allgemeinen Regeln des VwVG hinauszugehen. Zudem bleibt hier auch zu erwähnen, dass die betroffenen Personen auch auf zivilprozessualem Weg die Möglichkeit haben, entsprechende Massnahmen einzuleiten (vgl. Art. 28 ff. ZGB).
DSG	43			Der Beauftragte sollte diese Massnahmen nur ergreifen können, wenn er zuvor den Verantwortlichen beraten hat, es aber dennoch zu einer Verletzung kommt (im Sinne einer vorgängigen Abmahnung); i.V.m. Art. 44 VE-DSG haben die betroffenen Parteien Anspruch auf rechtliches Gehör (Art. 29 ff. VwVG), welcher hier zu gewähren ist. Wie bereits oben im Zusammenhang mit Art. 4 Abs. 4 und 5 VE-DSG (Grundsätze) und Art. 25 Abs. 3 VE-DSG (Rechtsansprüche) erwähnt, können zudem zwingende gesetzliche Vorschriften (z.B. Art. 958 f. OR oder Art. 7 GwG) oder gerichtliche, verwaltungsrechtliche oder aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter der Vernichtung oder Löschung von Personendaten entgegenstehen (vgl. obenstehende Ausführungen zu Art. 4 und Art. 25 VE-DSG). Anpassungsvorschlag (Ergänzungen unterstrichen): *Wenn Datenschutzvorschriften verletzt wurden, kann der Beauftragte verfügen, dass die Bearbeitung angepasst, ganz oder teilweise unterbrochen oder abgebrochen wird und die Daten ganz oder teilweise vernichtet werden, sofern zwingende gesetzliche Vorschriften oder gerichtliche, verwaltungsrechtliche oder*

				aufsichtsrechtliche Verfügungen oder berechtigte Interessen Dritter der Vernichtung nicht entgegenstehen.
DSG	46 f.			**Zusammenarbeit mit ausländischen Aufsichtsbehörden nach EU-DSGVO**: Gemäss EU-DSGVO sind Datenverantwortliche von Drittstaaten, die jedoch trotzdem der EU-Datenschutzgrundverordnung unterstehen, grundsätzlich zur Zusammenarbeit mit den Europäischen Aufsichtsbehörden verpflichtet. Ob eine Zusammenarbeit allerdings aus strafrechtlicher Sicht überhaupt zulässig ist, ist unklar (Art. 271 StGB – Verbotene Handlungen für einen ausländischen Staat). Hier wäre es wünschenswert, die Möglichkeiten der Amtshilfe (via den EDÖB bzw. die von uns unter Art. 50 ff. VE-DSG geforderte neue Verwaltungsbehörde) in das Gesetz zu übernehmen. Dann könnten Informationen über den Amtshilfeweg an die ausländischen Behörden übermittelt werden. Ausserdem besteht bereits durch das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarates eine Rechtsgrundlage, die den Weg der Amtshilfe und den Datenschutz entsprechend regelt (Art. 13 des Übereinkommens).
DSG	50 ff.			Art. 50 ff. VE-DSG enthalten eigentliche Strafbestimmungen, im Gegensatz zu den entsprechenden europäischen Regelungen, die Verwaltungssanktionen vorsehen. Bereits damit ist die mit dieser Gesetzesrevision bezweckte Äquivalenz gefährdet, da Verwaltungsverfahren eine effizientere Sanktionierung ermöglichen. Ein Wechsel vom Strafrecht hin zum Bundesverwaltungsrecht schafft eine rasche und kohärente Anwendung des Datenschutzgesetzes in der Praxis. Damit wird, wie bereits dargelegt, auf ein einheitliches und vor allem effizientes Verwaltungsverfahren hingewirkt. Verbleiben die Strafbestimmungen im Gesetz, so wird die Strafverfolgung automatisch an die Kantone delegiert. Damit ist kein einheitlicher Vollzug des Datenschutzgesetzes mehr möglich. Der Vollzug des Datenschutzrechtes in der Schweiz und damit auch die Sanktionierung von Verstössen ist aber klarerweise eine Bundesaufgabe. Bereits die bestehenden Strafbestimmungen im heutigen DSG haben nicht dazu beigetragen, die Vollstreckungspraxis des Datenschutzes zu vereinheitlichen. Es ist zudem ein Irrglaube, mit dem Abstützen auf das Strafrecht die Europäischen Vorgaben an den Datenschutz besser erfüllt zu haben. Dies führt zudem dazu, dass unter Strafrecht als Primat nicht die Unternehmen, sondern die einzelnen Individuen bestraft werden. Nach Art. 29 StGB setzt die strafrechtliche Haftung voraus, dass die betreffende natürliche Person (i) eine ihr obliegende Pflicht (ii) in einer der folgenden Eigenschaften verletzt hat:

				- als Organ oder Mitglied eines formellen (Bst. a) oder faktischen (Bst. d) Organs; - als Gesellschafter einer Personengesellschaft (Bst. b); - als Mitarbeiter mit selbständigen Entscheidungsbefugnissen im betreffenden Bereich (Bst. c). Der Kreis der von Strafe bedrohten Personen ist daher relativ weit gezogen. Ein Risiko strafrechtlicher Haftung hätten deshalb insbesondere - VR- und GL-Mitglieder der Gesellschaft; - VR- und GL-Mitglieder der Muttergesellschaft, falls sie bei der Tochter faktische Entscheidungskompetenzen in Anspruch nehmen; - Mitglieder einer Kollektivgesellschaft; - ggf. die für den Datenschutz eigenverantwortlichen Mitarbeiter im Rechtsdienst; - ggf. ein Compliance-Officer; - ggf. interne und externe Datenschutzbeauftragte. Gestützt auf die sehr offene Formulierung im VE-DSG wären aber letztlich sämtliche Mitarbeitenden von Strafsanktionen bedroht. Diese Tatsache, zusammen mit der extremen Unbestimmtheit der Straftatbestände (dazu unten), **führt zu einer durch nichts 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. Dies insbesondere auch wegen der Tatsache, dass geschäftliche Datenbearbeitungen notwendigerweise täglich stattfinden müssen. In scharfem Gegensatz zu den allermeisten anderweitig implementierten Strafnormen betreffen diejenigen gemäss VE-DSG demzufolge alltägliche Situationen, denen die natürlichen Personen gar nicht ausweichen können. Zudem fällt ins Gewicht, dass das Datenschutzgesetz ausschliesslich geschäftliche Datenbearbeitungen erfasst (vgl. oben Vorbemerkung II), die natürlichen Personen als Mitarbeitende des Unternehmens somit gestützt auf die geschlossenen Arbeitsverträge für das Unternehmen handeln. Auch deshalb erscheint das Primat der Belangung der natürlichen Personen als nicht sachgerecht. Folgerichtig liegt der vom VE-DSG

				gewählte Ansatz auch nicht auf der Linie zahlreicher anderer Gesetze mit spezialgesetzlichen Strafnormen, welche konsequenterweise zu Recht das Primat des Unternehmens statuieren (vgl. z.B. KG, UWG, FMG u. BEHG). Eine solch flächendeckende Pönalisierung eines Grossteils der schweizerischen Arbeitnehmer wäre **verfassungswidrig und weltweit einmalig**. Das europäische Recht sieht Sanktionen lediglich auf Ebene der Unternehmen vor. Solche Sanktionen wären auch ein klar überschiessender und mit Blick auf die zu erreichende Äquivalenz unnötiger und kontraproduktiver Swiss Finish. **Viele Pflichten des VE-DSG und damit auch die daraus abgeleiteten strafrechtlichen Tatbestände gemäss Art. 50 ff. VE-DSG sind überdies zu wenig konkret.** Art. 50 ff. VE-DSG erfüllen damit die strafrechtsdogmatische, im Verfassungsrecht begründete Regel von «nulla poena sine lege (stricta, certa)» offensichtlich nicht. Nur wenn aufgrund der Regel klar ist, welches konkrete Verhalten gefordert ist bzw. welche Unterlassung eine Verletzung darstellt, ist eine Sanktionierung zulässig. Strafrechtlich sanktionierbar dürfen mit Blick auf die weitreichenden Folgen und auf den Verhältnismässigkeitsgrundsatz jedenfalls zum Vornherein nur solche Pflichten sein, die (i) eine wesentliche Verbesserung des Datenschutzes bei den betroffenen Personen sicherstellen wollen und – kumulativ – (ii) genügend präzis formuliert sind, damit der Verantwortliche bzw. dessen Mitarbeitende durch geeignete Handlungsweisen, Implementierung geeigneter Massnahmen, etc. tatsächlich verhindern können, je mit strafrechtlichen Vorwürfen konfrontiert zu werden. Offene Sachverhalte wie z.B. «Informationspflichten», «Dokumentationspflichten» oder «Auskunftspflichten» können die skizzierten Anforderungen per definitionem nicht erfüllen, weil sie mit einem zu grossen Ermessensspielraum versehen sind. Vollends problematisch ist es nach dem Gesagten, trotz offenen Sachverhalten sogar fahrlässige Handlungsweisen strafrechtlichen Sanktionen unterstellen zu wollen. Mit dem vorgeschlagenen Strafrechtspaket wären die gesamte Wirtschaft und insbesondere die einzelnen natürlichen Personen, die als Angestellte von Unternehmen täglich mit Personendaten umzugehen haben, zu Unrecht mit unabsehbaren strafrechtlichen Risiken belastet. Dies hätte wohl massivste, heute noch gar nicht überblickbare Auswirkungen auf den Wirtschaftsstandort Schweiz. Die Abwanderung zahlreicher Unternehmen ins Ausland wäre eine mögliche Folge. Mit alldem würde das krasse Gegenteil von Äquivalenz erreicht. Solche Szenarien stünden auch in krassem Gegensatz zu aktuellen Anstrengungen in Bundesbern, ausländische Anbieter z.B. unter dem Thema FinTech anzuziehen, um damit die Wettbewerbsfähigkeit des Wirtschaftsstandorts Schweiz zu sichern und zu verbessern.

				Wir fordern deshalb, auf Strafrechtsartikel grundsätzlich zu verzichten und stattdessen den Verwaltungsbehörden eine angemessene Sanktionskompetenz einzuräumen. Dies entspräche den europäischen Parallelbestimmungen. Es wäre insbesondere deshalb sachgerecht, weil das Strafrecht primär natürliche Personen erfasst und das Unternehmensstrafrecht systembedingt nur als zusätzliches «Auffangbecken» zum Tragen kommen soll (vgl. Art. 53 VE-DSG). Wegen der Komplexität vieler datenschutzrechtlicher Setups (z.B. grenzüberschreitende Sachverhalte, zunehmender Trend zu Arbeitsteilung, etc.) ist es aber nicht angemessen, für die Implementierung eines suboptimalen datenschutzrechtlichen Setups einzelne natürliche Personen verantwortlich zu machen, dies sogar in strafrechtlich relevanter Form mit für eine Privatperson völlig unverhältnismässigen Bussen-Ansätzen. Vielmehr ist es sachgerecht und fairer, wenn stattdessen das zuständige Unternehmen wegen Organisationsmängeln – um die es bei der Datenschutz-Compliance ja gerade geht – die Verantwortung übernimmt. Mit dem Wechsel zu verwaltungsrechtlichen, durch die Verwaltungsbehörden verhängten Sanktionen wäre Art. 43 VE-DSG analog zum Kartellgesetz (KG) auszugestalten, allerdings im Gegensatz zum KG wegen den unterschiedlichen in Frage stehenden Rechtsgütern mit einem wesentlich tieferen Höchstbetrag (z.B. CHF 1 Mio.; vgl. oben zu Art. 17 VE-DSG). Da solche Sanktionen – anders als im Strafrecht – primär auf das Unternehmen zielen, kann damit das vorstehend skizzierte zentrale Thema, die primäre Haftung natürlicher Personen zu verhindern, angemessen geregelt werden. Dieses **Verwaltungsverfahren** ist wie folgt auszugestalten: a) Bei Verstössen gegen Datenschutzbestimmungen richten sich die Sanktionen grundsätzlich mit dem **Anknüpfungspunkt von Organisationsmängeln** direkt gegen die **Unternehmen**. b) Der **EDÖB** bleibt im Wesentlichen auf seine bisherigen Kompetenzen gemäss geltendem DSG beschränkt; stellt der EDÖB bei seinen eigenen Untersuchungen im Sinne einer Vorselektion grobe Datenschutzverletzungen fest, hat er die Untersuchung an eine (neu zu schaffende) **Spruchbehörde (DSG-«Kommission»)** in einem anderen Departement wie z.B. im EDI zu übertragen, welcher Untersuchungs- und Spruchkompetenz und falls nötig Verordnungskompetenz zukommt. Damit wird ein **rechtsstaatliches System** geschaffen, welches sich an der funktionalen Aufteilung zwischen Strafuntersuchungsbehörden und Strafgerichten anlehnt. Der finanzielle Zusatzaufwand für die Schaffung dieser Kommission wird durch die Einsparung von Aufwand beim EDÖB selbst und bei kantonalen Strafbehörden mehr als wettgemacht.

				c) Zur Sicherstellung der verfassungsmässigen Verfahrensgarantien darf es bei solchen Verwaltungsverfahren **keine Mitwirkungspflicht des Unternehmens** geben. d) Gegen Entscheide der Spruchbehörde steht der **Weg ans Bundesverwaltungsgericht** als Rechtsmittelinstanz offen. e) **Maximale Sanktion** gegen ein Unternehmen ist – wie im VE-DSG vorgesehen – eine **Busse von CHF 500'000.** Dieses Sanktionsmass ist auch im Lichte internationaler Vorgaben ausreichend. Da bei DSG-Verletzungen alltägliche Datenbearbeitungen im Fokus stehen, welche typischerweise auch nur eine einzelne natürliche Person betreffen, verbieten sich insbesondere massiv höhere, i.d.R. umsatzbezogene Sanktionsansätze wie z.B. unter dem KG. Dort haben sanktionierte Unternehmen typischerweise jahrelang von kartellistischen Machenschaften finanziell massiv profitiert, was im Einzelfall höhere Bussen zu rechtfertigen vermag (zumal selbst diese höheren Bussen i.d.R. nur einen Teil des unrechtmässig erzielten Gewinns zurückholen). Unter dem DSG gibt es demgegenüber kaum Gewinn zu erzielen, weil die Datenbearbeitungen ohnehin stattfinden müssen. f) Lediglich **subsidiär** ist parallel zu oder anstatt einem gegen das Unternehmen gerichteten Verwaltungsverfahren eine strafrechtliche Verfolgung von **klar kriminellen Mitarbeitenden** möglich. Dies jedoch mit folgenden Beschränkungen: (i) Beschränkung der Delikte auf solche Handlungen, welche eine direkte Schädigung bei betroffenen Personen bewirken können; (ii) Strafbarkeit auf direkten Vorsatz beschränkt (sonst besteht das Risiko, dass auf Basis der Organisationspflichten des Unternehmens allzu schnell Eventualvorsatz «konstruiert» wird); und (iii) Recht zum Strafantrag nur für ein betroffenes Unternehmen. g) Generell sind die **Straftatbestände zu konkretisieren** und auf ein vernünftiges und mit den strafrechtlichen Prinzipien konformes Mass einzugrenzen, insb. durch (i) Streichung der Strafandrohung bei verweigerter Mitwirkung / Kooperation ab der zweiten Stufe des Verfahrens; (ii) Konkretisierung / Streichung der zu offen formulierten Tatbestände; (iii) Einführung einer Erheblichkeitsschwelle, welche sich z.B. an der Schwere der Persönlichkeitsverletzung (in quantitativer oder qualitativer Hinsicht) oder an der Höhe des entstandenen Schadens orientiert; zu einem schweren Verstoss gegen das Datenschutzgesetz gehört auch, dass die unbefugte Datenbearbeitung direkt vorsätzlich vorgenommen wurde; (iv) Verzicht auf die Pönalisierung von reinen Fahrlässigkeitsdelikten; und (v) Beschränkung des allgemeinen Berufsgeheimnisses auf Fälle, in

				denen der Geheimnisherr eine berechtigte Erwartung der Geheimhaltung hat (z.B. aufgrund eines Vertrages). Art. 35 DSG ist beizubehalten, eventualiter ist der Tatbestand mindestens auf das Niveau von Art. 321 StGB zu relativieren. h) Das Zusammenspiel der Pflicht, Datenschutzverstösse zu melden, mit der damit einhergehenden anschliessenden Bestrafung im Rahmen eines Strafverfahrens verstösst gegen das Selbstbelastungsverbot (nemo tenetur) und ist unfair, weil sie die korrekt handelnden Personen, welche ihren Meldepflichten nachkommen, dafür bestraft. Umgekehrt werden falsche Anreize gesetzt, denn andere Personen, welche bewusst die Meldepflicht nicht befolgen, können nach dem natürlichen Lauf der Dinge ernsthaft damit rechnen, dass der Fall nicht publik wird und sie demzufolge straffrei bleiben. Deshalb sollte ein kooperatives Verhalten im Sinne einer Schadensminderung gefördert werden. Dies muss durch einen gesetzlich anerkannten Katalog angemessener **Rechtfertigungsgründe** geschehen. Solche Fallgruppen fairer Rechtfertigungsgründe sind insb. (i) Einhaltung der Corporate Governance: Einhalten sämtlicher unternehmensinternen Regulative, Ausschöpfen der betriebsinternen Eskalationsleiter und Interventionsmöglichkeiten, Meldung eines möglichen Verstosses sowie kooperatives Verhalten gegenüber den Behörden; (ii) Handeln nach Treu und Glauben durch vernünftigen Umgang mit komplexen Regeln: Angemessene Umsetzung komplexer Verhältnisse (u.a. viele Beteiligte und grenzüberschreitende Verhältnisse) unter Berücksichtigung des «state of the art» und bei bestehender Rechtsunsicherheit; (iii) Wahrung berechtigter Interessen: Rechtfertigende Pflichtenkollision mit anderen zwingenden Rechtsregeln, welche in einer Güterabwägung im konkreten Fall überwogen haben. Beispielsweise unter Zeitdruck angewendete etablierte Notfallszenarien (BCM) im öffentlichen Interesse der Abwendung eines Unternehmenskonkurses (vgl. Notstand, Art. 17 StGB); (iv) Strafrechtliche Verfolgung eines Mitarbeiters: Eine Anzeige gegen einen direkt vorsätzlich handelnden Mitarbeiter durch das Unternehmen muss im Rahmen der Bestrafung des Unternehmens, insbesondere im Hinblick auf das Schuldprinzip, berücksichtigt werden; und (v) Aktive Schadensverminderung und damit die aktive Zusammenarbeit mit den Behörden im Falle einer Verletzung. Auch die von uns als Ersatz für Strafrechtstatbestände geforderten verwaltungsrechtlichen Sanktionen sind genügend präzis im weiter vorne skizzierten Sinn zu formulieren.

DSG	51	2		Absatz 2 sollte **ersatzlos gestrichen** werden, ansonsten könnte jeder Verantwortliche bei jedem Entscheid, der sich als nicht richtig herausstellt, bereits gebüsst werden. Dies würde zu einer Kriminalisierung sämtlicher Verantwortlichen führen.
DSG	51bis (neu)			In Anlehnung an Art. 83 Abs. 3 EU-DSGVO regen wir für den Eventualfall an, mit Art. 51bis VE-DSG einen neuen Artikel mit dem Titel «Konkurrenz» einzufügen. Formulierungsvorschlag: *Konkurrenz* *Hat eine private Person bei der gleichen oder bei miteinander verbundenen Datenbearbeitungsvorgängen vorsätzlich oder fahrlässig mehrere Bestimmungen dieses Gesetzes verletzt, so übersteigt der Gesamtbetrag der Busse nicht den Betrag der für die schwerwiegendste Verletzung vorgesehen ist.*
DSG	52			Die **Abgrenzung zu anderen gesetzlich geregelten Geheimhaltungspflichten** ist unklar. Unterschiedliche Regelungen in verschiedenen Gesetzen im Bereich strafrechtlich relevanter Handlungen schaffen Rechts*un*sicherheit und unnötige Abgrenzungs- und Auslegungsprobleme und widersprechen damit auch strafrechtlichen Grundprinzipien. Die Regelung strafrechtlicher Tatbestände auf solche, bereits grundsätzlich unklarer Regelungen ist verfassungsrechtlich unzulässig (Verletzung des Grundsatzes nulla poena sine lege stricta). Umso mehr ist Art. 52 VE-DSG zu streichen (vgl. oben zu Art. 50 ff. VE-DSG).
DSG	53			Es ist wichtig, dass diese Bestimmung, wenn schon, nicht als Kann-Vorschrift ausgestaltet ist, ansonsten es sehr schwierig sein wird, qualifizierte Personen zu finden, die sich für eine Anstellung unter solchen Bedingungen zur Verfügung stellen. Anpassungsvorschlag: *Übertretungen und Vergehen in Geschäftsbetrieben* *Von der Ermittlung der strafbaren Personen wird ~~kann~~ Umgang genommen und an ihrer Stelle der Geschäftsbetrieb zur Bezahlung der Busse verurteilt.~~werden Busse 100 000 Franken nicht überschreitet und~~

				~~*die Ermittlung der Personen, die nach Artikel 6 des Bundesgesetzes vom 22. März 1974 über das Verwaltungsstrafrecht strafbar sind, Strafuntersuchungsmassnahmen bedingt, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären*~~
DSG	54			Da dies bereits in der Strafprozessordnung geregelt ist, ist diese Bestimmung jedenfalls obsolet und ersatzlos zu streichen.
DSG	55			Da dies bereits in Art. 109 des Strafgesetzbuches geregelt ist, ist diese Bestimmung jedenfalls obsolet und ersatzlos zu streichen.
DSG	59			Die Übergangsbestimmungen von Art. 59 VE-DSG beschränken sich auf die Regelungen von Art. 16, 18 u. 19 VE-DSG. In Tat und Wahrheit lässt sich der gegenüber dem bestehenden DSG wesentlich veränderte und mit zahlreichen veränderten bzw. neuen Pflichten ausgestattete VE-DSG nur im Zuge einer **umfassenden IT-gestützten Umstellung der gesamten internen Datenbearbeitungsprozesse** bewerkstelligen. Dies geht weit über Art. 16, 18 u. 19 VE-DSG hinaus und umfasst sämtliche geänderten oder neuen Pflichten und anderen, zur Strukturierung der rechtskonformen Datenbearbeitung notwendigen Regeln. Nur schon für einfache Umsetzungsprojekte sind auf der Zeitachse **zwischen Analyse, Entscheidfindung und IT-gestützter massengeschäftstauglicher Umsetzung erfahrungsgemäss rund zwei Jahre Übergangsfrist** notwendig. Mit Blick auf die **Komplexität des neuen VE-DSG** mit Bezug auf die zahlreichen zur rechtskonformen Umsetzung notwendigen Anpassungen an sämtlichen Datenbearbeitungsprozessen sind dafür **im Minimum drei Jahre** absolut zwingend.
DSG	59	b		Es ist kein Grund ersichtlich, weshalb vom gesetzgeberischen **Grundsatz der Nichtrückwirkung** abgewichen werden soll. Die Datenbearbeitungen bis zum Inkrafttreten des VE-DSG erfolgten rechtskonform auf Basis des aktuellen DSG und sämtlicher anderen anwendbaren Gesetze und wurden überdies auch von den zuständigen Prüfgesellschaften periodisch geprüft. Auch das aktuelle DSG statuiert bereits zahlreiche Informationspflichten. Auch die in Art. 18 u. 19 Bst. b VE-DSG neu formulierten Pflichten finden sich in anderer Systematik bereits im geltenden DSG. Deshalb erscheint eine Rückwirkung als Ausnahme von der Regel nicht angemessen. Die Rückwirkung würde in der praktischen Umsetzung zudem einen enormen Aufwand und überdies zahlreiche kaum lösbare Herausforderungen generieren. Bei langjährigen Kunden würde schlussendlich eine Information erheblichen Ausmasses generiert, welche die meisten Kunden überdies kaum mehr

				interessieren würde, weil z.B. die Datenbearbeitung viele Jahre zurückliegt, heute gar nicht mehr zur Anwendung kommt, u.ä. Sämtliche Kunden müssten – als Erben früherer Kunden – auch über längst zurückliegende Datenbearbeitungen informieren, welche nur schon wegen dem inzwischen verstorbenen Erblasser nach Jahr und Tag kaum mehr von Interesse sein dürften. Zahlreiche Informationen zur Wahrnehmung solcher nachträglichen Informationspflichten wären ohnehin nicht mehr vorhanden, weil sie inzwischen nach Ablauf der Archivierungs- und anderweitigen Aufbewahrungspflichten gar nicht mehr vorhanden sind. Die allermeisten betroffenen Personen würden solche nachträglichen Informationen mit einigem Erstaunen zur Kenntnis nehmen und könnten damit kaum etwas Vernünftiges anfangen, sondern wären eher verwirrt. Im dümmsten Fall würden sich zahlreiche Kunden und andere betroffene Personen auf der Basis der erhaltenen Informationen beim verantwortlichen Unternehmen melden und zusätzliche Fragen stellen. Der Aufwand für die Unternehmen wäre massiv, ohne dass damit ein wesentlicher datenschutzrechtlicher Mehrwert geschaffen würde. Nach dem Gesagten ist Art. 59 Bst. b VE-DSG **ersatzlos zu streichen** und die Systematik des verbleibenden Art. 59 VE-DSG anzupassen und als vollständiger Satz zu formulieren (da eine einzelne Bst. a keinen Sinn mehr macht).
GwG	34	2		Vgl. Anmerkungen zum unten vorgeschlagenen Art. 34bis. Anpassungsvorschlag (Ergänzungen unterstrichen): *Sie dürfen Daten aus diesen Datensammlungen nur an die FINMA, die Eidgenössische Spielbankenkommission, Selbstregulierungsorganisationen, die Meldestelle und Strafverfolgungsbehörden weitergeben. <u>Vorbehalten bleibt die Weitergabe an Zweigniederlassungen und innerhalb einer Finanzgruppe gemäss Artikel 34bis.</u>*
GwG	34bis (neu)			Die FINMA konkretisiert das per 2016 in Kraft getretene revidierte Geldwäschereigesetz sowie die entsprechende GwV-FINMA dahingehend, dass ein Finanzintermediär, der Zweigniederlassungen im Ausland besitzt oder der eine Finanzgruppe mit ausländischen Gesellschaften leitet, seine mit Geldwäscherei und Terrorismusfinanzierung verbundenen Rechts- und Reputationsrisiken global erfassen, begrenzen und überwachen muss (Art. 6 Abs. 1 GwV-FINMA). Art. 6 Abs. 2 Bst. a und b GwV-FINMA setzt bei der Pflicht zur gruppenweiten Erfassung, Begrenzung und Überwachung von Risiken

				im Bedarfsfall den Zugang der zuständigen Überwachungsorgane der Gruppe zu Informationen über einzelne Geschäftsbeziehungen voraus. Die Bestimmungen des Geldwäschereigesetzes sind daher dahingehend zu ergänzen, dass der Informationsaustausch innerhalb der Finanzgruppe im In- und Ausland zulässig ist, falls und soweit dieser zur Erfüllung der Pflichten aus dem GwG erforderlich ist. Dies entspricht auch der in Präambel (19) der EU-DSGVO festgehaltenen Bestimmung, wonach die Mitgliedstaaten Erlasse beschliessen können, welche die in der EU-DSGVO festgehaltenen Pflichten und Rechte beschränken, soweit dies zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung erforderlich und verhältnismässig ist. Formulierungsvorschlag: *Weitergabe an Zweigniederlassungen und innerhalb einer Finanzgruppe* *Sofern zur Erfüllung der in diesem Gesetz festgelegten Pflichten erforderlich, darf der Finanzintermediär, der Zweigniederlassungen besitzt oder Teil einer Finanzgruppe ist, Informationen an Zweigniederlassungen und andere Rechtseinheiten innerhalb der Finanzgruppe im In- und Ausland weitergeben. Davon eingeschlossen sind sämtliche für die globale Überwachung der Rechts- und Reputationsrisiken wesentlichen Informationen, inklusive Informationen über einzelne Geschäftsbeziehungen und Informationen aus Datensammlungen gemäss Art. 34.*
ZPO	20 99 113 114 243	d 3 2 2	d d g f d	Wir verlangen die ersatzlose Streichung der Änderungen in der ZPO. Betroffen davon sind die Gerichtsstandbestimmungen, Sicherheiten und Gerichtskosten. Als speziell stossend betrachten wir den Umstand, dass ein neuer Gerichtsstand für Datenschutzstreitigkeiten eingeführt wird. Weshalb im Rahmen der Datenschutzgesetzgebung die Streitwertgrenzen in der Zivilprozessordnung aufgehoben werden sollen ist uns ebenfalls nicht ersichtlich. Generell besteht kein sachlicher Grund, für Datenschutzbelange von den bewährten Regeln der ZPO abzuweichen. Letztere müssen aus Gründen von Klarheit und Übersichtlichkeit Grundregel bleiben. **Ausnahmen** davon sind nur für **zwingend notwendige Spezialsituationen** zuzugestehen. Solche liegen im Bereich Datenschutz nicht vor und werden dementsprechend im Erläuterungsbericht auch nicht angeführt.

Geschäftsstelle

Wallstrasse 8
Postfach
CH-4002 Basel

Telefon 061 206 66 66
Telefax 061 206 66 67
E-Mail vskb@vskb.ch

Verband Schweizerischer Kantonalbanken
Union des Banques Cantonales Suisses
Unione delle Banche Cantonali Svizzere

Wir bedanken uns für die wohlwollende Prüfung unserer Bemerkungen und Anliegen. Für allfällige Rückfragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Verband Schweizerischer Kantonalbanken

Hanspeter Hess
Direktor

Dr. Adrian Steiner
Leiter Public Affairs