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

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

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

Stellungnahme von

Name / Firma / Organisation	: Schweizer Dialogmarketing Verband (SDV)
Abkürzung der Firma / Organisation	: SDV
Adresse	: Postfach 616, 8501 Frauenfeld
Kontaktperson	: RA Lukas Bühlmann
Telefon	: 052 721 61 62
E-Mail	: info@sdv-dialogmarketing.ch; buehlmann@br-legal.ch
Datum	: 31. März 2017

Wichtige Hinweise:

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

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

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

Herzlichen Dank für Ihre Mitwirkung!

Inhaltsverzeichnis

Allgemeine Bemerkungen 3

Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vorentwurf) 5

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

Entwurf zur Revision des Übereinkommens SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten Fehler! Textmarke nicht definiert.

Erläuternder Bericht (ohne Kapitel 8 "Erläuterungen zu den einzelnen Artikeln") Fehler! Textmarke nicht definiert.

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln" 28

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

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

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

Allgemeine Bemerkungen

Name/Firma	Bemerkung/Anregung
SDV	Wir begrüssen die mit dem vorliegenden Entwurf angestrebte Modernisierung des Datenschutzrechts und die beabsichtigte Annäherung an die künftige Rechtslage in der EU. Im rasanten Wandel des technologischen Umfelds ist es für unsere Verbandsmitglieder, wie auch für alle anderen Unternehmen, zentral, dass mit der künftigen Regelung Rechtssicherheit für die wirtschaftliche Tätigkeit geschaffen wird. Diese Anforderung ist umso wichtiger, als mit der Revision das Sanktionssystem erheblich verschärft werden soll. Unklarheiten sind daher so weit wie möglich zu vermeiden. Zugleich müssen die Einschränkungen der wirtschaftlichen Freiheit und die administrativen Aufwendungen, die den Unternehmen durch die Änderung der rechtlichen Vorgaben entstehen, auf das absolut Notwendige reduziert werden. Ferner räumt der Bundesrat der Aufrechterhaltung der Angemessenheit des Schweizer Datenschutzrechts zwar zu Recht eine hohe Priorität ein. Zu beachten ist dabei jedoch, dass es hierfür keinesfalls erforderlich ist, über die Vorgaben der E-SEV 108 und der EU-DSGVO hinauszugehen. Leider enthält der Vorentwurf zahlreiche Bestimmungen, die gegenüber den internationalen Verpflichtungen der Schweiz zu verschärften Vorschriften für Schweizer Unternehmen enthält. Dies führt zu Standortnachteilen für in der Schweiz ansässige Unternehmen. Vor diesem Hintergrund lehnen wir im Grundsatz jegliche Änderungen gegenüber der geltenden Rechtslage ab, die zur Einhaltung der Vorgaben der Europarats-Konvention (E-SEV 108) oder mit Blick auf die Angemessenheits-Beurteilung des Schweizer Datenschutzrechts durch die EU nicht zwingend geboten sind (sog. Swiss Finish). Angesichts der Tatsache, dass Datenbearbeitungen bereits heute häufig und künftig noch vermehrt grenzüberschreitend erfolgen, können Schweizer Sonderregelungen in Abweichung der EU-DSGVO, welche die unternehmerische Tätigkeit und die Zusammenarbeit zwischen nationalen Behörden erschweren, nicht gutgeheissen werden. Ausgehend davon sind insbesondere der „Swiss Finish“ bei der vorgeschlagenen Regelung des „Profiling“ und der Sanktionierung von Verstössen strikt abzulehnen. Diese, aber auch zahlreiche weitere punktuelle Bestimmungen, auf die wir nachgehend eingehen, bedürfen daher einer grundlegenden Überarbeitung. In der aktuellen Fassung müssen wir den vorgelegten Vorentwurf des neuen DSG ablehnen. Insbesondere das vorgesehene Sanktionssystem, mit dem eine weitgehende Kriminalisierung von natürlichen Personen in den datenbearbeitenden Unternehmen anstelle einer direkten Disziplinierung der wirtschaftlich verantwortlichen Unternehmen erfolgt ist inakzeptabel. Dieses Sanktionssystem führt zudem zu einer massiven Bevorteilung international tätiger Grossunternehmen gegenüber Schweizer Unternehmen, da die Verfolgung und Vollstreckung gegenüber im Ausland ansässigen Unternehmen faktisch und rechtlich nicht möglich sein wird. Es ist sodann auch in besonderem Masse KMU-feindlich, da die Rechtsverfolgung der entsprechend sanktionierten Tatbeständen gegen verantwortliche Personen in kleineren Organisationen viel einfacher und damit für die kantonalen Strafverfolgungsbehörden viel „effizienter“ möglich wäre.. Darüber hinaus ist zwar der Verzicht auf die zwingende Einführung eines betrieblichen Datenschutzbeauftragten zu begrüssen. Allerdings ist die

	freiwillige Einführung eines solchen zu unterstützen, weshalb das Institut gesetzlich weiter vorgesehen sein sollte. Unternehmen, die einen Beauftragten einführen, sollten ferner von gewissen Meldepflichten befreit werden. Zudem müsste dies bei der Sanktionierung angemessen berücksichtigt werden.

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

Name/Firma	Gesetz	Art.	Abs.	Bst.	Bemerkung/Anregung
SDV	DSG	1			Entsprechend der Strategie des Bundesrats für eine „digitale Schweiz“ und den Zielsetzungen in der EU-DSGVO ist der Zweck der „Förderung des freien Verkehrs von Personendaten“ in die Bestimmung aufzunehmen.
SDV	DSG	2	1		Im Hinblick auf die Annäherung an die Regelung in der EU-DSGVO und aufgrund der damit verbundenen Erleichterung von Datentransfers ins Ausland ist die Ausklammerung von juristischen Personen grundsätzlich zu begrüssen.
SDV	DSG	3		a	Die Beibehaltung der Definition von Personendaten ist zu begrüssen. Unter Einbezug des erläuternden Berichts ist die vorgeschlagene Regelung jedoch unklar und potentiell widersprüchlich. Auf der einen Seite soll der Begriff „Personendaten“ gemäss Bericht gegenüber dem geltenden Recht zwar inhaltlich nicht geändert werden**. Dabei ist insbesondere die implizite Anerkennung der relativen Methode, wie sie auch in der EU künftig weiterhin gelten soll, zentral und richtig**. Auf der andern Seite wird im Bericht jedoch eine natürliche Person als bestimmbar erklärt, wenn sie „über Hinweise auf eine Identifikationsnummer oder eine Online-Identität“ identifiziert werden kann. Diese Formulierung ist gerade in diesem für sämtliche Online-Aktivitäten fundamentalen Punkt missverständlich und je nach Interpretation widersprüchlich. Denn nach der wohl herrschenden Auffassung genügt es unter dem geltendem DSG nicht, wenn Angaben bloss einer bestimmten „eindeutigen Kennung“ oder „Identifikationsnummer“, wie z.B. einer IP-Adresse oder Cookie-Kennungen zugeordnet werden können, hinter welcher letztlich eine Person steht, diese aber nicht namentlich identifiziert werden kann (sog. Singularisierung). Bei der

					Qualifikation von IP-Adressen etc. muss daher auch künftig eine Einzelfallbeurteilung entscheidend sein, unter Berücksichtigung des Aufwands zur Identifizierung mit den zur Verfügung stehenden technischen Möglichkeiten (objektive Seite) sowie dem Interesse an der Identifizierung (subjektive Seite). Insbesondere beim Einsatz von Cookies zur Auslieferung von individualisierter Werbung auf Websites, bei welchem regelmässig auch die IP-Adresse mitbearbeitet wird, besteht dabei kein Interesse an der namentlichen Identifikation des Nutzers, sondern lediglich an der Kategorisierung. Würde hier stets von Personendaten ausgegangen werden müssen**, hätte dies erhebliche Auswirkungen auf die gesamten Online-Aktivitäten, sodass letzten Endes zahlreiche heute werbefinanzierte, unentgeltliche Angebote künftig nicht mehr allgemein zur Verfügung stehen würden. Vor diesem Hintergrund ist eine Klarstellung in der Botschaft, dass das Konzept der Singularisierung abgelehnt wird, von zentraler Bedeutung.** Der Umstand, dass nach Auffassung einzelner Autoren unter der EU-DSGVO eine Singularisierung für das Vorliegen von Personendaten ausreichen soll, ändert daran nichts. Denn zum einen wird diese Auffassung von anderen Autoren mit überzeugenden Argumenten abgelehnt. **Zum anderen ergibt sich eine derart strenge Auslegung auch nicht aus dem E-SEV 108. Deshalb besteht keine Notwendigkeit, sie im Schweizer Recht einzuführen (Swiss Finish).**
SDV	DSG	3		c. 4.	Der Begriff der biometrischen Daten ist zu präzisieren: Besonders schützenswert sollen nur biometrische Daten sein, die zum Zweck der Identifizierung bearbeitet werden. Bilder in Zeitungen wären damit ausgenommen (der vorgesehene Wortlaut würde dazu führen, dass solche Bilder unter den Begriff der „biometrischen Daten“ fallen.
SDV	DSG	3		f	**Die vorgeschlagene Definition und die damit einhergehende Regelung (siehe dazu Anmerkungen zu Art. 23 unten) des „Profiling“ werden abgelehnt. Die Definition geht ohne Not weit über diejenige der EU-DSGVO**

					(Art. 4 Ziff. 4) hinaus (Swiss Finish). Zudem enthält der E-SEV 108 keinerlei Vorgaben für das Profiling. Vielmehr verlangt dieser nur eine Regelung von automatisierten Entscheidungen (vgl. Art. 8 Abs.1 lit. a). Ausgehend davon sollte auf spezifische Vorgaben für das Profiling verzichtet werden. Wird gleichwohl an einer Regelung festgehalten, sollte diese aber **jedenfalls auf automatisierte Bearbeitungen beschränkt bleiben. Keinesfalls darf die Regelung jedoch derart weit gefasst werden, dass die Vorgaben (systemwidrig) sogar für das Profiling mit nicht personenbezogenen Daten gelten.** Für die im erläuternden Bericht angesprochenen Bearbeitungen bspw. im Rahmen von Big Data Analysen genügen die übrigen Regelungen vollends. Denn bei einem Profiling, das am Ende zu Personendaten führt, gelten diese ohnehin bereits. Darüber hinaus wird die Unsicherheit, welche konkreten Bearbeitungen in der Praxis als Profiling zu betrachten sind, durch den entsprechenden Zusatz weiter verstärkt.
SDV	DSG	4			Das Festhalten an den bestehenden Datenbearbeitungsgrundsätzen ist im Allgemeinen zu begrüssen.
SDV	DSG	4	3		Das Erfordernis der „klaren“ Erkennbarkeit ist zu streichen. Da eine Änderung der geltenden Rechtslage hiermit nicht beabsichtigt und eine solche auch nicht erforderlich ist, sorgt der Zusatz lediglich für Unsicherheit.
SDV	DSG	4	5		Beibehaltung des geltenden Art. 5 Abs. 1 DSG. Gemäss Seite 47 des Erläuterungsberichts sind hier keine materiellen Änderungen beabsichtigt. Konsequenterweise ist der bisherige Wortlaut beizubehalten, sonst wird nur neue Unsicherheit geschaffen. Eventualiter: Beschränkung von Abs. 5 auf den Satz "Wer Personendaten bearbeitet, muss überprüfen, ob die Daten richtig sind", Streichung des Restes dieses Passus'. Bekanntlich fängt die "Bearbeitung" ja schon bei der Aufbewahrung an (vgl. Art. 3 lit. d VE). Eine fortdauernde Verpflichtung zur

					Nachführung wäre offensichtlich unerfüllbar. "Unvollständig" muss ebenfalls gestrichen werden. Es ist nicht möglich, allen künftigen Veränderungen des Status' einer Person nachzugehen, über die zu einem bestimmten Zeitpunkt Daten bearbeitet worden sind. Schliesslich ist ausdrücklich klarzustellen, dass die Pflicht nur den Verantwortlichen trifft. Nur der Verantwortliche ist in der Lage, allfälligen Änderungsbedarf zu erkennen.
SDV	DSG	4	6		**Die vorgeschlagene Änderung hinsichtlich des überaus zentralen Begriffs der „Einwilligung“ ist unter Einbezug des erläuternden Berichts unklar.** Gemäss erläuterndem Bericht (S. 47) ermöglicht die Neuformulierung eine terminologische Annäherung an die DSGVO. Es wird allerdings nicht klargestellt, ob damit eine inhaltliche Annäherung bezweckt wird. Die Definition ist nicht nur, aber in besonders ausgeprägter Form gerade für die Werbebranche von fundamentaler Bedeutung, weshalb eine klare Regelung und damit Rechtssicherheit erforderlich ist**. Die Übernahme der gegenüber der E-SEV 108 unnötig strengen Vorgaben der EU-DSGVO in Bezug auf die „Freiwilligkeit der Einwilligung“ (Art. 7 Abs. 4) hätte jedenfalls eine massive Verschärfung der Rechtslage gegenüber dem geltenden Recht sowie eine erhebliche Beschränkung der Vertragsfreiheit zur Folge, die unnötig und daher abzulehnen ist.** Der E-SEV 108 (Art. 5 Abs. 2) verlangt denn auch lediglich, dass die Einwilligung freiwillig sein muss („free consent“), ohne eine derart strenge Interpretation, wie sie die EU-DSGVO enthält, vorzuschreiben. **In der Botschaft muss deshalb eine entsprechende Klarstellung aufgenommen werden**. **Darüber hinaus sind die Ausführungen im erläuternden Bericht zur „ausdrücklichen Einwilligungen“ unklar bzw. unvollständig.** Es geht daraus letztlich nicht hervor, welche Anforderungen konkret an eine solche Einwilligung gestellt werden, was gerade aufgrund des (noch) übermässig weit gefassten Begriffs des Profiling und dessen Bedeutung für die Werbebranche besonders problematisch ist**. Es ist daher in der Botschaft auch klar zu stellen, dass – wie nach geltendem Recht – eine Einwilligung dann ausdrücklich ist, wenn**

					die Datenbearbeitung, in welche eingewilligt wird, also z.B. das Profiling, bspw. in der Datenschutzerklärung beim Namen genannt wird und es insofern genügen würde, wenn bloss aus den Umständen auf ein Profiling geschlossen werden müsste. Schliesslich ist in der Botschaft auch festzulegen, dass – entsprechend dem geltenden Recht – **eine Einwilligung in Datenbearbeitungen auch durch Zustimmung zu einem Dokument, das weitere Informationen erhält (wie z.B. AGB oder Datenschutzerklärungen), erteilt werden kann** und keine separate Information bzw. Einwilligung erforderlich ist.
SDV	DSG	5	3-6		**Die Regelung zur Bekanntgabe ins Ausland bei fehlendem Angemessenheitsbeschluss in verschiedener Hinsicht anzupassen**. Insbesondere geht die Regelung vereinzelt weiter als diejenige der EU-DSGVO **(Swiss Finish).** Generell ist die Unterscheidung zwischen spezifischen und standardisierten Garantien unklar. Es sollte einzig zwischen Standardverträgen und anderen Verträgen/Garantien unterschieden werden. Ferner ist analog der EU-DSGVO die Pflicht zur Information des EDÖB in Art. 5 Abs. 6 VE-DSG zu streichen. Denn es erscheint zweifelhaft, ob und inwiefern eine entsprechende Information letztlich zum Datenschutz beiträgt. Zudem ist die Genehmigungsfrist in Art. 5 Abs. 5 VE-DSG unverhältnismässig lang und kontraproduktiv. Schliesslich ist auch die Ausdehnung der Pflichten auf Auftragsdatenbearbeiter abzulehnen.
SDV	DSG	6	1	b	**Auch an dieser Stelle geht die Regelung unnötig über diejenige der EU-DSGVO (Art. 49 Abs. 1 lit. c) hinaus (Swiss Finish).** Deshalb muss eine Bekanntgabe ins Ausland auch dann erlaubt sein, wenn ein Vertrag lediglich im Interesse der betroffenen Person abgeschlossen worden ist.
SDV	DSG	6	2		Die Informationspflicht bei Vorliegen eines Ausnahmetatbestands ist weder in der EU-DSGVO noch im E-SEV 108 vorgesehen. Die Bestimmung ist daher zu

					streichen.
SDV	DSG	7			Die grundsätzliche Beibehaltung der geltenden Rechtslage hinsichtlich der Auftragsdatenbearbeitung ist zu begrüssen. **Abzulehnen ist jedoch die vorgesehene Ausdehnung der Vergewisserungspflicht dahingehend, ob die Bearbeitung durch den Auftragsbearbeiter die Rechte der betroffenen Personen gewährleisten kann.** Diese Ausdehnung der Vergewisserungspflicht ist unklar und würde zu erheblichem Mehraufwand für das Outsourcing führen. Der Auftragsbearbeiter ist nie der Ansprechspartner der betroffenen Personen. Vielmehr müsste sichergestellt sein, dass der Auftragsbearbeiter das Erforderliche dafür tut, dass der Verantwortliche die Rechte der betroffenen Personen gewährleisten kann. **Zu verzichten ist auch auf die unbeschränkte Delegation an den Bundesrat zur Festlegung weiterer Pflichten. Zudem ist Abs. 3 zu streichen.** Eine zwingende Zustimmung zum Beizug von Sub-Auftragsdatenbearbeiter ist weder durch die internationalen Verpflichtungen gefordert, noch entspricht sie der bisher geltenden Rechtslage (**Swiss Finish**). Sie wäre in der Praxis auch nicht praktikabel. Sollte daran festgehalten werden, müsste die Bestimmung zumindest dahingehend angepasst werden, dass nicht „Schriftlichkeit“ erforderlich ist, sondern eine Form, die den „Nachweis durch Text“ ermöglicht. Andernfalls wäre die Ermächtigung zur Einsetzung von Unterauftragnehmern namentlich in Verträgen, die Online abgeschlossen werden, nicht mehr möglich.
SDV	DSG	8			Die vorgeschlagene Regelung und die Einführung von Empfehlungen der guten Praxis ist im Grundsatz zu begrüssen. Allerdings kann das Genehmigungsverfahren nicht dem EDÖB alleine unterliegen. Die Genehmigungsinstanz ist genau zu definieren und zu erweitern. **Generell muss jedoch klargestellt werden, wer zu den interessierten Kreisen gehört.** Eine Mitwirkung von Konsumentenverbänden ist auszuschliessen, da deren Interessen bereits durch den Genehmigungsvorbehalt

					des EDÖB ausreichend berücksichtigt werden. Schlussendlich muss gegen die Entscheide des EDÖB, resp. der Genehmigungsinstanz ein Rechtsmittel gegeben sei.
SDV	DSG	8	1		Die Kompetenz des EDÖB zum eigenständigen Erlass von Empfehlungen ist in mehrerer Hinsicht problematisch und deshalb zu streichen. So bestünde die Gefahr, dass der EDÖB letztlich im Alleingang ohne ausreichende Berücksichtigung der branchenspezifischen Bedürfnisse und Besonderheiten Empfehlungen erlässt. Die entsprechenden Empfehlungen dürften in der Regel einen über die gesetzlichen Vorgaben hinausgehenden Standard setzen, der faktisch, trotz der sinnvollen Klarstellung in Art. 9 Abs. 3 VE-DSG, zum Gesetz wird. Darüber hinaus erscheint fraglich, ob es sich dabei um Verfügungen handelt. Sofern die Regelung beibehalten würde, müsste den betroffenen Unternehmen jedenfalls eine Anfechtung ermöglicht werden. Es wäre demnach eine klare Regelung der Rechtsmittel im Gesetz selbst erforderlich.
SDV	DSG	8	2		Nach einem allfälligen Entscheid über die Genehmigung von Empfehlungen wird sich stets die Frage nach den Rechtsmitteln und insbesondere nach der Legitimation zur Ergreifung eines solchen stellen. Zur Klärung der Rechtslage wären hier zumindest Erläuterungen in der Botschaft angezeigt. Die Rechtsmittel, welche allgemein auch im E-SEV 108 verlangt werden (Art. 12bis Abs. 6), sind umso mehr von Bedeutung, als aufgrund der Pflicht zur Genehmigung durch den EDÖB zu erwarten ist, dass mit den Empfehlungen ein über die gesetzlichen Vorgaben hinausgehender Standard gesetzt wird. Dieser wird letztlich auch trotz der expliziten Regelung in Art. 9 Abs. 2 VE-DSG faktisch zum Gesetz werden. **Folglich muss eine klare Regelung bestehen, die es den betroffenen Verbänden bzw. Unternehmen ermöglicht, die Nicht-Genehmigung bzw. Ablehnung einer Empfehlung, die den gesetzlichen Vorgaben entspricht, gerichtlich anzufechten.**

SDV	DSG	12			Die Einführung einer Regelung zu Daten verstorbener Personen ist im Hinblick auf die Angemessenheit des Schweizer Datenschutzrechts nicht zwingend erforderlich und führt für die Unternehmen zu einem erheblichen administrativen Mehraufwand **(Swiss Finish)**. **Auf die Regelung ist daher zu verzichten**. Andernfalls sollte sie zumindest sinnvoll eingeschränkt werden. Insbesondere muss es Unternehmen möglich sein, sich auf überwiegende eigene Interessen oder gesetzliche Pflichten zu berufen, wenn ihnen gegenüber Rechte verstorbener geltend gemacht werden. Erben dürfen im Verhältnis zu einem Datenbearbeiter jedenfalls nicht über mehr Rechte verfügen als der Erblasser zu Lebzeiten selbst.
SDV	DSG	13			Die Einführung einer generellen Informationspflicht ist mit Blick auf den E-SEV 108 zwingend und insofern richtig**. Allerdings gehen diverse Punkte der vorgeschlagenen Regelung zu weit und sind daher abzulehnen** (vgl. dazu nachfolgend). Unklar ist danach ferner, inwiefern die Informationspflicht auch gilt, wenn nachträglich neue Bearbeitungszwecke hinzukommen oder andere Bearbeitungen an die Stelle der ursprünglichen treten. Diesbezüglich ist eine Klarstellung erforderlich, dass nur über das informiert werden muss, was schon zum Zeitpunkt der Beschaffung feststand bzw. dass sich die Information auf den Zeitpunkt der Beschaffung bezieht. Denn in solchen Fällen wäre in der Regel ohnehin eine Einwilligung oder ein anderer Rechtfertigungsgrund erforderlich und eine Sanktionsbewehrung folglich unverhältnismässig. Eine Pflicht zur Nachinformation ist klar auszuschliessen. **Zudem muss zwingend müsste klargestellt werden, dass – entsprechend der geltenden Rechtslage und der Praxis des EDÖB – bei der Beschaffung grundsätzlich ein Verweis auf die auf der Website enthaltenen Detailinformationen ausreicht.** Die Erwägung im erläuternden Bericht, wonach es nicht genügt, wenn die betroffene Person nach den Informationen suchen muss, sollte deshalb zumindest im Rahmen der Botschaft in diesem Sinne

					präzisiert werden.
SDV	DSG	13	2		Angesichts der Sanktionsdrohung sollte eine abschliessende Aufzählung der mitzuteilenden Informationen erfolgen. Andernfalls würden sich Unternehmen zur Vermeidung von Risiken dazu gezwungen sehen, den betroffenen Personen die Vielzahl der Informationen, wie sie in der EU-DSGVO vorgesehen sind, mitzuteilen. Den Betroffenen wäre mit einer solchen Vielzahl von Informationen letztlich nicht gedient. Sie führt nicht zu mehr, sondern im Ergebnis zu weniger Transparenz. Die Mitteilungspflichten gemäss EU-DSGVO gehen über den durch die SEV-108 vorgegebenen Standard hinaus **(Swiss Finish)**. Hier ist eine abschliessende, schlanke Aufzählung vorzusehen. Zudem ist hinsichtlich des Zeitpunkts der Information für den Online-Kontext eine Klarstellung erforderlich. Denn beim Zugriff auf eine Website wird regelmässig eine Bearbeitung von IP-Adressen erfolgen (Erfassung in Log-Datei, Zählung der Website-Zugriffe etc.) und dies in der Regel bereits bevor der Nutzer allfällige Informationen hierzu z.B. in einer Datenschutzerklärung zur Kenntnis nehmen kann. Aufgrund der Tatsache, dass IP-Adressen je nach Einzelfall Personendaten darstellen können und dass eine vorgängige Information hier technisch grundsätzlich nicht möglich ist, **muss klargestellt werden, dass die ausreichend kenntlich gemachte Information in einer Datenschutzerklärung nach Abruf der Website als rechtzeitig gilt.**
SDV	DSG	13	4		Diese Vorgabe hinsichtlich der Information bei einer Auftragsdatenbearbeitung ist weder im E-SEV 108 noch in der EU-DSGVO vorgesehen **(Swiss Finish)**. Sie ist daher ersatzlos zu streichen, da sie für den Betroffenen keinerlei Mehrwert bringt.
SDV	DSG	13	5		Die Ausdehnung der Pflicht auf die indirekte Datenbeschaffung wird in der Praxis jegliche Beschaffung von Daten bei Dritten verunmöglichen. Die Bestimmung ist daher zu streichen. Sofern daran festgehalten wird, ist zu beachten, dass der Entwurf auch hier über die Vorgaben der EU-DSGVO hinausgeht. Analog der EU-Regelung (Art. 14 Abs. 3) müsste es daher in jedem Fall für die

					Datenbeschaffung bei Dritten auch in der Schweiz zulässig sein, die Information zu späteren Zeitpunkten zu erteilen.
SDV	DSG	14			**Der Katalog der Ausnahmen ist enger gefasst, als es nach dem E-SEV 108 erforderlich wäre (Swiss Finish)**. So ist insbesondere der einschränkende Zusatz „*und er die Personendaten nicht Dritten bekannt gibt*“ in Art. 14 Abs. 4 lit. a zu streichen. Solange ein überwiegendes Interesse des Verantwortlichen besteht, ist nicht einzusehen, wieso die Ausnahme nicht gelten soll, wenn Personendaten an Dritte bekannt gegeben werden. Darüber hinaus ist auch Art. 14 Abs. 3 lit. a zu eng gefasst, da sich konkrete Bearbeitungen selten „ausdrücklich“ aus dem Gesetz selbst ergeben. Schliesslich ist auch Abs. 5 zu streichen, da die Umsetzung dieser Vorgabe in der Praxis, insbesondere hinsichtlich überwiegenden Interessen, zu einem unverhältnismässigen Aufwand führt und nicht praktikabel ist. Schliesslich sind hier auch weitere Ausnahmen vorzusehen, um einer missbräuchlichen Geltendmachung des Auskunftsrechts entgegenzuwirken.
SDV	DSG	15			Der Anwendungsbereich der Informations- und Anhörungspflicht ist viel zu weit gefasst, indem gemäss den Erläuterungen bereits „beliebige rechtliche Wirkungen“ genügen. Hier müsste **klargestellt werden, dass auch rechtliche Auswirkungen eine gewisse Schwere erreichen müssen.** Die Regelung zu automatisierten Einzelfallentscheidungen geht zudem wiederum unverständlicherweise über die Vorgaben der EU-DSGVO (Art. 22) hinaus **(Swiss Finish)**. Die dort vorgesehenen Ausnahmen müssen ebenfalls übernommen werden. **Eine derart strenge Regelung ist jedenfalls auch nach dem E-SEV 108 nicht erforderlich.**
SDV	DSG	16			**Die Anknüpfung an das Vorliegen „erhöhter Risiken“ führt zu einem viel zu weit gefassten Anwendungsbereich und geht unverständlicherweise über die Vorgaben in der EU-DSGVO (Art. 35) hinaus (Swiss Finish)**.Der Entwurf und die Erläuterungen bleibt denn auch unklar, was ein „erhöhtes Risiko“ sein

					soll. Jedes noch so kleine Risiko kann als „erhöht“ gegenüber keinem Risiko angesehen werden. Diese Formulierung ist schon deshalb untauglich und zu streichen. Bleibt es bei dieser Formulierung, würde diese zu einem übermässigen Aufwand führen, der sowohl für die Unternehmen als auch für den EDÖB nicht zu bewältigen ist. Denn, wie aus dem erläuternden Bericht hervorgeht, könnte eine solche Pflicht zur Datenschutz-Folgeabschätzung letztlich bei jeder Übermittlung in Länder wie die USA, jedem Profiling und jeder Bearbeitung von besonders schützenswerten Daten bestehen. Dies würde für die Werbebranche zu massiven Kosten führen, da die Pflicht bspw. auch für das Profiling zur Einblendung personalisierter Werbung oder beim Web-Tracking bestehen würde. Entsprechend der EU-Regelung **sollte daher zumindest auf Datenbearbeitungen mit „hohem Risiko“ (oder besser „besonders hohem Risiko“) abgestellt werden**. Dabei sollten auch diejenigen Fälle, in denen die Pflicht besteht, (zumindest beispielhaft) konkretisiert und Ausnahmen vorgesehen werden. Ausgenommen werden sollten namentlich Fälle, in welchen die Betroffenen mit den Datenbearbeitungen einverstanden sind. **Des Weiteren ist die Bezugnahme auf die Risiken für die „Grundrechte“ von Betroffenen bei Datenbearbeitungen durch Private unpassend und folglich zu streichen.** Die vorgeschlagene Regelung geht sodann auch in weiteren Punkten über die EU-DSGVO hinaus **(Swiss Finish)**: So ist die Pflicht entsprechend der EU-Vorschriften (Art. 35 DSGVO) auf den Verantwortlichen zu beschränkt. Eine Ausdehnung auf den Auftragsdatenbearbeiter ergibt letztlich keinen Sinn. Darüber hinaus ist, wenn überhaupt, nur dann eine Meldepflicht gegenüber dem EDÖB vorzusehen, wenn trotz der getroffenen Schutzvorkehrungen nach Auffassung des Verantwortlichen gleichwohl ein „hohes Risiko“ besteht. Mehr verlangt auch die EU-DSGVO nicht (Art. 36 Abs. 1). Mit der vorgeschlagenen Regelung wäre die Meldepflicht derart weit gefasst, dass der Aufwand wiederum weder durch die Unternehmen noch den EDÖB

					bewältigt werden kann. **Schliesslich ist auch die Frist von drei Monaten zur Beurteilung durch den EDÖB länger als diejenige in der EU-DSGVO (Art. 36 Abs. 2). Das Abwarten dieser Frist nicht praktikabel und führt zu einer erheblichen Einschränkung der Handlungsfreiheit der Unternehmen und letztlich zu einer Lähmung der Wirtschaft. Die Frist muss daher entsprechend erheblich verkürzt werden.**
SDV	DSG	17	1		**Nach der vorgeschlagenen Regelung besteht gegenüber dem EDÖB grundsätzlich für jede „unbefugte Datenbearbeitung“ eine Meldepflicht**. Daher hat eine Meldung im Grundsatz bei jedem auch noch so geringfügigen Verstoss zu erfolgen. Dabei handelt es sich wiederum um ein **schweizerisches Überschiessen (Swiss Finish),** welches zudem viel weiter geht, als zum Schutz der Betroffenen erforderlich ist. Die vorgesehene Einschränkung auf Fälle, die voraussichtlich nicht zu einem „Risiko für die Persönlichkeit“ des Betroffenen führen, vermag den Anwendungsbereich sodann auch nicht hinreichend zu begrenzen. Entsprechend der Vorgabe im E-SEV 108 (Art. 7 Abs. 2**) ist die Meldepflicht daher auf Verletzungen zu beschränken, welche die Rechte der Betroffenen „schwerwiegend“ („seriously“) gefährden könnten.** In diesem Sinne sollte die Meldepflicht wie auch in der EU-DSGVO auf Fälle beschränkt werden, die zu einem Bruch oder Verlust des Gewahrsams an Daten führen. Bei der vorgeschlagenen Meldepflicht zeigt sich ferner auch deutlich, dass die vorgesehene Sanktionsregelung, welche auf die Bestrafung natürlicher Personen fokussiert, falsch ist. So werden Mitarbeiter vollkommen unangebracht in eine Drucksituation versetzt, sofern sie Kenntnis von einer Verletzung erlangen: Entweder denunzieren sie den zuständigen Mitarbeiter oder machen sich andernfalls unter Umständen gar selbst strafbar. Dies hätte nachhaltige Auswirkungen auf die interne Organisation und Governance rund um datenschutzrechtliche Risiken innerhalb eines Unternehmens. Dieses müsste letztlich immer damit rechnen, dass einzelne Mitarbeiter entsprechende Meldungen machen. Aufgrund der persönlichen strafrechtlichen Verantwortung der Mitarbeiter könnten auch keine Vorgaben an die Ausübung der

					entsprechenden Meldepflichten gemacht werden. Die Pflicht zur Selbstanzeige, die hier eingeführt werden soll, ist unserem Rechtssystem völlig fremd. Der Grundsatz, sich nicht selbst belasten zu müssen, gehört zu den zentralen Verfahrensgarantien. Wieso dieser im Bereich des Datenschutzes plötzlich nicht mehr gelten soll, ist völlig unerfindlich; dies umso weniger, als der Beauftragte gemäss Art. 45 VE ja seinerseits verpflichtet ist, allfällige strafbare Handlungen zur Anzeige zu bringen (sofern am strafrechtlichen Sanktionssystem festgehalten werden sollte). Der Verantwortliche müsste sich m.a.W. nicht nur an das datenschutzrechtliche, sondern auch noch an das strafrechtliche Messer liefern. Im Übrigen dürfte es für die Verantwortlichen oftmals schwierig sein, zu entscheiden, ob effektiv eine Datenschutzverletzung vorliegt. Aufgrund der drastischen Strafdrohungen, mit welcher der VE Verletzungen (auch) dieser Verpflichtung sanktionieren will, wäre mit einer regelrechten Flut an Selbstanzeigen zu rechnen, die nur den Apparat des Beauftragten übermässig aufblähen würde.
SDV	DSG	17	2		Wiederum als Schweizer Sonderregelung abzulehnen ist die Meldepflicht gegenüber Dritten. Eine derart weitgehende und aufwändige administrative Zusatzbelastung ist auch in der EU-DSGVO (Art. 19) nicht vorgesehen. Die Pflicht ist auf Fälle zu beschränken, in welchen der betroffenen Person ein schwerwiegender, nicht wiedergutzumachender Nachteil droht..
SDV	DSG	18			Die Einführung dieser neuen Pflichten (Privacy by Default und Privacy by Design) ist namentlich deshalb problematisch, weil deren Verletzung unmittelbar sanktioniert werden soll. Bei beiden Pflichten gibt es nicht eine einzige richtige Vorgehensweise. Nach dem vorgeschlagenen Wortlaut sind „angemessene Massnahmen“ bzw. „geeignete Voreinstellungen“ vorzunehmen. **Hier muss den Datenbearbeitern im Sinne der „Business Judgement Rule“ ein gewisser Ermessensspielraum eingeräumt werden. In der Botschaft ist dies**

					klarzustellen. Ansonsten wäre die Sanktionierung insbesondere auch mit Blick auf das strafrechtliche Bestimmtheitsgebot problematisch. Schliesslich werden die Pflichten wiederum in Abweichung von der EU-DSGVO (Art. 25) ohne ersichtlichen Grund auch den Auftragsbearbeitern auferlegt, für welche die Vorgaben in der Praxis kaum umsetzbar sind. Die Pflichten sind deshalb auf die Verantwortlichen zu beschränken.
SDV	DSG	19			Der vorgeschlagene Entwurf geht auch hier unverständlicherweise über die die Vorgaben der EU-DSGVO hinaus (Art. 19 und 30), indem die Pflichten, nicht nur dem Verantwortlichen auferlegt werden **(Swiss Finish)**. Die Auftragsbearbeiter sind hier in jedem Falle in Bezug auf die in Art. 19 Abs. 2 VE-DSG vorgesehene Informationspflicht aus der Pflicht zu nehmen.
SDV	DSG	19		a	Die vorgeschlagene Dokumentationspflicht ist zu weit gefasst und führt für Unternehmen zu einem erheblichen und unnötigem Aufwand. **Die Regelung darf keinesfalls über das in der EU-DSGVO (Art. 30) vorgeschriebene Verzeichnis der Datenbearbeitungen hinausgehen.** Damit ein solches Verzeichnis überhaupt seinen Zweck erfüllen kann, muss es jedenfalls auf regelmässige Datenbearbeitungen beschränkt sein, andernfalls müsste bereits jegliche Korrespondenz darin erfasst werden. Darüber hinaus sind, wie auch im Rahmen der EU-DSGVO (Art. 30 Abs. 5), entsprechende Ausnahmen vorzusehen. In der aktuell vorgesehenen Form stellt auch diese Bestimmung ein schweizerisches Überschiessen **(Swiss Finish)**.
SDV	DSG	19		b	**Eine solche Mitteilungspflicht ist im E-SEV 108 nicht vorgesehen (Swiss Finish). Sie ist deshalb ersatzlos zu streichen.** Sofern an ihr festgehalten werden sollte, dann ist die Pflicht zur Mitteilung von Berichtigungen, Löschungen oder Vernichtungen von Personendaten im aktuellen Entwurf zu weit gefasst. **Es bedarf hier einer zusätzlichen Einschränkung, wonach eine Mitteilung nur erfolgen muss, wenn die betroffene Person ein schützenswertes Interesse hat**. Zudem geht die

					vorgeschlagene Regelung **wiederum unverständlicherweise über die Vorgaben der EU-DSGVO (Art. 19) hinaus, indem Verletzungen des Datenschutzes auch den Empfängern offen gelegt werden müssen (Swiss Finish)**. Schliesslich ist auch eine zeitliche Beschränkung vorzusehen, sodass nur Empfänger informiert werden müssen, wenn die Daten während einer gewissen Frist weitergegeben wurden (z.B. innert der letzten 5 Jahre, gerechnet vom Zeitpunkt der Informationspflicht).
SDV	DSG	20	1		**Die Anforderung der Kostenlosigkeit des Auskunftsrechts ergibt sich nicht aus dem E-SEV 108 und ist zu streichen (Swiss Finsih)**. Im Gegenteil wird nur verlangt, dass die Auskunftserteilung ohne übermässige Kosten zu erfolgen hat („without excesive expense"; Art. 8 Abs. 1 lit. b). Folglich muss es den Unternehmen möglich sein, **eine angemessene Aufwandsentschädigung** zu verlangen. Die Auswirkungen der Kostenlosigkeit insbesondere auf KMU-Unternehmen darf nicht unterschätzt werden. Sie kann durchaus eine existentielle Bedrohung darstellen, sollte davon inskünftig extensiver Gebrauch gemacht werden. Es ist davon auszugehen, dass diese Rechte inskünftig zunehmend und in einem intensiveren Ausmass genutzt werden, als bislang. Hier ist die Einschätzung von PWC im Rahmen der Regulierungsfolgeabschätzung in besonderem Ausmass unrealistisch.
SDV	DSG	20	3		**Das Auskunftsrecht hinsichtlich von Entscheidungen aufgrund einer automatisierten Datenbearbeitung ist viel zu weit gefasst und nach der vorgeschlagenen Regelung geradezu uferlos.** Entsprechend der Regelung in der EU-DSGVO (Art. 15 Abs. 1 lit. h) ist das Auskunftsrecht auf diejenigen Fälle zu beschränken, in welchen auch eine Informations- und Anhörungspflicht nach Art. 15 VE-DSG besteht, also auf Entscheidungen, die automatisiert erfolgen und entsprechende Auswirkungen haben. Die aktuell vorgesehene Regelung ist wiederum unnötig überschiessend **(Swiss Finish)** und ist zwingend einzuschränken.

SDV	DSG	23			**Das generelle Erfordernis der ausdrücklichen Einwilligung für das Profiling stellt eine der problematischsten Schweizer Verschärfungen dar und ist zwingend zu streichen (Swiss Finish)**. Für die Werbewirtschaft hat diese Anforderung erhebliche Konsequenzen, welche unnötig sind. Denn nach dem E-SEV 108 ist eine entsprechende Vorgabe nicht verlangt. Ferner ist auch nach der EU-DSGVO nicht für jegliche Form des Profiling eine Einwilligung erforderlich. Aber auch in der Sache besteht keine Notwendigkeit, das Profiling per se als Persönlichkeitsverletzung einzustufen. Solange die Datenbearbeitungsgrundsätze eingehalten werden, ist nicht ersichtlich, wieso neben der Information stets zusätzlich auch eine Einwilligung erforderlich sein soll. **Wird diese Vorschrift Gesetz, verunmöglicht sie faktisch einem grossen Teil der in der Schweiz ansässigen Unternehmen jede Form von personalisierter Werbung / Marketing und stellt eine Bedrohung für den Standort Schweiz dar**. Profiling und damit personalisierte Werbung wäre dann nur noch den grossen (insbesondere internationalen) Log-in Giganten wie Facebook, Google, Apple und Co. vorbehalten. Diese Unternehmen können sich meist problemlos auf eine ausdrückliche Einwilligung im Rahmen der Account-Registrierungen stützen. Das Ergebnis wäre sodann auch aus kartellrechtlichen Überlegungen höchst problematisch.
SDV	DSG	23	3		Die Beibehaltung der geltenden Regelung von allgemein zugänglich gemachten Daten ist zu begrüssen. Dabei ist jedoch die Erwägung im erläuternden Bericht, wonach die Regelung nur zum Tragen komme, wenn die Bearbeitung dieser Daten auch rechtmässig erfolgt (S. 69), unzutreffend und daher in der Botschaft klar zu stellen.
SDV	DSG	24	2		**Die Neuformulierung, wonach die aufgezählten Sachverhalte bloss „möglicherweise“ ein überwiegendes Interesse darstellen, ist abzulehnen.** Zweck der Aufzählung ist die Schaffung von Rechtssicherheit. Mit der neuen

					Formulierung wird diese aber sogleich wieder aufgehoben. Der SDV fordert sodann, dass entsprechend der EU-DSGVO (Erw.-Gr. 47) zumindest in der Botschaft darauf hinzuweisen ist, dass die Bearbeitung von Personendaten zum Zwecke der Direktwerbung ein überwiegendes Interesse darstellen kann.
SDV	DSG	24	2	a.	**Das Wort „unmittelbar“ ist zu streichen**. Es führt zu einer zu starken Einschränkung und lässt unnötigen Interpretationsspielraum.
SDV	DSG	24	2	C3	**Volljährigkeit: Absatz 2 lit. c (3) ist ersatzlos zu streichen.** Eine Volljährigkeit kann häufig erst mit einer Datenprüfung festgestellt werden (oder eben auch nicht). Hier ist die Formulierung so zu wählen, dass es bei einer Kreditprüfung Pflicht ist, die Volljährigkeit zu prüfen. Online-Versandhändler führen in den meisten Fällen für den Kauf auf Rechnung eine Kreditprüfung durch. Dabei ist Volljährigkeit ein entscheidendes Merkmal für das Zustandekommen des Vertrages. Zudem bestehen diverse Umstände, die eine Prüfung auf Volljährigkeit gesetzlich erforderlich machen. Die Durchführung einer Kreditprüfung ist häufig das zuverlässigste Mittel zur Prüfung der Volljährigkeit.
SDV	DSG	25			Zu begrüssen ist das grundsätzliche Festhalten am bisher bewährten zivilrechtlichen Rechtschutz und namentlich der Verzicht auf eine besondere Regelung des „Rechts auf Vergessen“. Das geltende Recht gewährt bereits ausreichende und ausgewogene Möglichkeiten, um sich gegen eine Datenbearbeitung zur Wehr zu setzen. **Allerdings ist der letzte Satz in Absatz 2 ersatzlos zu streichen**. Weder die E-SEV 108 noch die DSGVO sehen vor, dass neben dem Bestreitungsvermerk auch eine Beschränkung der Datenbearbeitung verlangt werden kann. Die Umsetzung dieser überschiessenden neuen Bestimmung **(Swiss Finish)** ist nicht praktikabel.

SDV	DSG	37-49			Die erforderliche Anpassung des Sanktionssystems (Verwaltungs- anstelle von Strafsanktionen, siehe unten) bedingt auch eine Überarbeitung der vorgeschlagenen Regelungen zum EDÖB. Zur Vermeidung einer zu grossen Machtfülle durch Bündelung von Untersuchungs- und Spruchkompetenzen und zur Ermöglichung einer vertrauensvollen Kooperation zwischen Unternehmen und EDÖB ist eine Datenschutz-Kommission zu bilden, welche über Verfügungs- und Sanktionskompetenzen verfügt. Der EDÖB hätte in dieser Struktur seine bisherigen Aufgaben wahrzunehmen und namentlich eine Vorselektion der ihm zugetragenen Fälle durchzuführen. Bei Verdacht auf einen Verstoss, würde er die Angelegenheit an die Datenschutz-Kommission weiterleiten. Auf dieser Stufe des Verfahrens ist auch auf eine Mitwirkungspflicht der Unternehmen zu verzichten (Stichwort: Selbstbelastungsverbot). Zur Anfechtung der Entscheide der Kommission müsste ein Rechtmittel vor Bundesverwaltungsgericht ergriffen werden können. Im Übrigen verweisen wir auf die ausführlichen entsprechenden Stellungnahmen in der Vernehmlassungsantwort der economiesuisse.
SDV	DSG	44	3		**Unabhängig vom letztlich gewählten Modell ist jedenfalls eine Regelung abzulehnen, wonach vorsorgliche Massnahmen der zuständigen Behörde per se keine aufschiebende Wirkung haben sollen.** Da die Einstellung oder Anpassung von Datenbearbeitungen während der ungewiss langen Dauer des Verwaltungsverfahrens **massive und durchaus auch irreparable Schäden** für die Unternehmen verursachen kann, muss den Betroffenen zumindest die Möglichkeit gegeben werden, die Erteilung der aufschiebenden Wirkung durch die zuständige Rechtsmittelinstanz zu beantragen.
SDV	DSG	50 ff.			**Das vorgeschlagene Sanktionssystem, das primär auf die persönliche strafrechtliche Verurteilung von natürlichen Personen abstellt, wird strikt abgelehnt**. Dieses vorgesehene Sanktionssystem steht der Digitalen Strategie der Schweiz diametral entgegen. Es ist in höchstem Mass innovationshemmend und etabliert eine Kultur des Denunziantentums in den Unternehmen. Es führt zu einem ganz erheblichen Standortnachteil der Schweiz. Kein innovatives digitales

					Start-Up wird bereit sein, seine Gründer und Mitarbeiter solch drastischen strafrechtlichen Risiken auszusetzen. Gute Mitarbeiter werden nicht mehr bereit sein Verantwortung in den Unternehmen mitzutragen. Insbesondere aufgrund der vorgesehenen Strafbarkeit fahrlässigen Verhaltens wird potentiell jeder Mitarbeiter durch heute alltägliche Verrichtungen am Arbeitsplatz ständig Gefahr laufen, sich strafbar zu machen. Dies ist auch gesellschaftspolitisch komplett inakzeptabel. Gleichzeitig ist es gegenüber Datenbearbeitungen durch ausländische Unternehmen faktisch nicht durchsetzbar, was sodann einerseits den Datenschutz in der Schweiz nicht erhöht und andererseits ausländischen Unternehmen einen immensen Wettbewerbsvorteil verschafft. Sodann würde die Schweiz damit gegenüber der EU in diesem grundlegenden Punkt einen Sonderweg einschlagen. Selbst wenn gemäss dem E-SEV 108 nicht zwingend administrative Bussen verlangt werden, wird gleichwohl eine unnötige Unsicherheit im Hinblick auf die Beurteilung der Angemessenheit des Schweizer Datenschutzrechts geschaffen. Ferner wird die Abweichung wie erwähnt international aber auch schon im europäischen Kontext zu vollstreckungsrechtlichen Schwierigkeiten führen (Stichwort: Voraussetzung der doppelten Strafbarkeit), was letztlich zu einer Bevorzugung von ausländischen Unternehmen gegenüber den einheimischen führt. **In jedem Falle wird die vorgeschlagene Regelung aber auch die für die Schweizer Wirtschaft zentralen Verhandlungen zwischen der Schweiz und der EU über die Koordinierung der Anwendung des jeweiligen Datenschutzrechts und die Abgrenzung der Zuständigkeit der Aufsichtsbehörden (Motion Fiala, 16.3752) erheblich erschweren.** Es erscheint gänzlich unrealistisch, dass die EU eine entsprechende Vereinbarung abschliesst, wenn in der Schweiz Unternehmen, die Datenschutzverletzungen gegenüber EU-Bürgern begehen, nur in Ausnahmefällen bzw. nach Ermessen der Untersuchungsbehörden verfolgt werden können.

					Darüber hinaus greift auch die Begründung „mit Blick auf die Kosten“ im erläuternden Bericht viel zu kurz. Die Kosten werden mit der vorgeschlagenen Regelung lediglich auf die kantonalen Strafbehörden übertragen. Es ist nicht ersichtlich, inwiefern sich diese hierdurch verringern sollten. Im Gegenteil ist ein solches **System ineffizient und wird gesamtwirtschaftlich deutlich höhere Kosten verursachen**, da neben dem Verwaltungsverfahren des EDÖB bei Verdacht auf strafrechtlich relevante Verhaltensweisen ein zusätzliches Strafverfahren mit neuerlichen Untersuchungsmassnahmen durchzuführen ist. Der gleiche Fall müsste folglich zweimal untersucht werden. Dies würde auch für die Unternehmen zu einem nicht vertretbaren und unnötigen Mehraufwand führen. **Schliesslich ist auch die primäre strafrechtliche Sanktionierung der natürlichen Personen an sich unverhältnismässig und mit Blick auf den Datenschutz nicht zielführend.** Die betroffenen Mitarbeiter würden durch das Risiko einer strafrechtlichen Verurteilung massiv unter Druck gesetzt. Namentlich bei Kenntnis einer Verletzung müssten sie entweder den zuständigen Mitarbeiter denunzieren oder würden sich andernfalls unter Umständen gar selbst strafbar machen. Ferner besteht die Gefahr, dass Unternehmen nach Möglichkeit einen unliebsamen Mitarbeiter im Sinne eines „Bauernopfers“ für den massgeblichen Verstoss als zuständig bezeichnen und sich so letztlich aus der Verantwortung nehmen können. **Zudem würde gerade die Position von betrieblichen Datenschutzverantwortlichen, die eigentlich zur Erhöhung des Datenschutzes beitragen sollten, mit dem vorgeschlagenen System erheblich geschwächt.** Statt der Förderung des betrieblichen Datenschutzes würde damit eine Kultur der Verschleierung geschaffen. Insbesondere in kleineren Unternehmen, in welchen die zuständige Person einfacher ausfindig zu machen ist, dürfte kaum mehr jemand bereit sein, eine entsprechende Stelle, resp. die entsprechende Verantwortung zu übernehmen.

					Geradezu absurd erscheint die Schärfe des vorgeschlagenen Sanktionssystems, wenn man bedenkt, dass damit ausgerechnet der materielle Kern eines wirksamen Datenschutzes, nämlich die Beachtung der Bearbeitungsgrundsätze, nicht sanktionsbedroht sein soll. Dies im Übrigen natürlich zu Recht. Spätestens in diesem Zusammenhang wird nämlich klar, dass sich das Strafrecht als disziplinierendes Instrument in diesem Bereich nicht eignet. In einem Rechtsstaat kann ein Verhalten nur strafbar sein, wenn der zugrundeliegende Tatbestand eindeutig bestimmt ist. Gerade dies ist aber im Bereich des Datenschutzes in den meisten Fällen nicht der Fall: wie soll ein Mitarbeiter voraussehen können, ob die mit einer Bearbeitung verbundenen Risiken genügend „erhöht“ sind, um damit die strafrechtlich sanktionierte Pflicht einer Risiko-Folgenabschätzung im Sinne von Art. 16 VE-DSG auszulösen? **Vor diesem Hintergrund sind anstelle von Strafsanktionen verwaltungsrechtliche Bussen einzuführen.** Für Binnensachverhalte ist es allerdings nicht angezeigt, die Bussenrahmen der EU-DSGVO zu übernehmen. Hier genügen tiefere Maximalsanktionen. Mit Blick auf eine allfällige Koordinations-Vereinbarung mit der EU sollten die Obergrenzen für Verstösse, die den EU-Markt betreffen, allerdings höher ausfallen. Der SDV schliesst sich der Forderung der economiesuisse nach einem Sanktionssystem entsprechend den folgenden Grundsätzen an: Die Sanktionen sollen sich primär an die Unternehmen richten und verwaltungsrechtlicher Natur sein. Eine Sanktionierung von Mitarbeitenden ist nur für Fälle von direkt vorsätzlichen Verstössen vorzusehen, in welchen sich das Handeln des Mitarbeiters gegen die Interessen des Unternehmens oder der betroffenen Person richtet. Der Kreis der potentiell verantwortlichen Mitarbeitenden muss dabei klar definiert und angemessen eingeschränkt werden. Des Weiteren ist der Strafkatalog anzupassen. Dieser darf in keinem Fall über die EU-DSGVO hinausgehen. Zu offen formulierte Tatbestände sind dabei entweder

					aus dem Katalog zu entfernen oder zu konkretisieren. Zudem ist eine Erheblichkeitsschwelle einzuführen, die sich an der Schwere der Persönlichkeitsverletzung oder an der Höhe des entstandenen Schadens orientiert. Auf die Sanktionierung von fahrlässig begangenen Verstössen ist zu verzichten. Schliesslich ist auch kooperatives Verhalten durch geeignete Anreize zu fördern, indem Sanktionen bei Vorliegen von schadensminderndem Verhalten wegfallen oder zumindest reduziert werden. Im Übrigen verweisen wir auf die ausführliche Stellungnahme der economiesuisse in deren Vernehmlassungsantwort.
SDV	DSG	52			**Der vorgeschlagene Ausbau der geltenden Regelung (Art. 35 DSG) ist abzulehnen.** Ein berechtigter Grund oder die Notwendigkeit hierfür besteht nicht. Sofern die Regelung extensiv interpretiert wird, würde die Konzeption des Schweizerischen Datenschutzrechts auf den Kopf gestellt werden – zumindest betreffend die Bekanntgabe von Daten an Dritte. Bis anhin durften „normale“ Personendaten grundsätzlich ohne einen Rechtfertigungsgrund an Dritte weitergegeben werden – sofern auch die anderen Datenbearbeitungsgrundsätze eingehalten wurden. Nur für besonders schützenswerte Personendaten und Persönlichkeitsprofile wurde vermutet, dass die Bekanntgabe an Dritte ohne Zustimmung der betroffenen Person eine Persönlichkeitsrechtsverletzung darstellt. Art. 52 VE-DSG würde diesen Mechanismus auf den Kopf stellen. Obwohl eigentlich der materielle Teil des Datenschutzgesetzes für die Bekanntgabe von normalen Personendaten an Dritte keinen Rechtfertigungsgrund verlangt, würde eine solche Pflicht zumindest bei der Bekanntgabe von „geheimen“ Personendaten über den Umweg der strafbewehrten Schweigepflicht eingeführt werden. Eine solche Umkehr des geltenden Mechanismus ist nicht begründet und wird auch weder von der E-K108 verlangt, noch ist eine entsprechende Pflicht in der DSGVO vorgesehen. Hier schiesst der Vorentwurf damit klar und ohne Not über das Ziel hinaus. **Hinzu kommt, dass der Begriff der „geheimen Personendaten“ unklar ist. Letztlich würde damit ein allgemeines**

					Berufsgeheimnis für jedermann geschaffen, wonach praktisch jeder Berufstätige einer Geheimhaltungspflicht unterstehen würde, was unverhältnismässig ist.
SDV	DSG	55			Sollte es bei der strafrechtlichen Sanktionen bleiben, so ist die Verjährungsfrist auf 3 Jahre zu reduzieren. Dies entspricht Art. 109 StGB und wäre ausreichend und sachgerecht (auch im Verwaltungsverfahren).
SDV	ZPO	99	3	d	Der SDV lehnt die Abschaffung der Möglichkeit einer Sicherstellungspflicht für die Parteientschädigung der beklagten Partei ab. Es ist fragwürdig, die Konkretisierung der datenschutzrechtlichen Normen und damit die Rechtssicherheit über eine Incentivierung zivilrechtlicher Streitigkeiten erreichen zu wollen. Diese Konkretisierung ist in erster Linie Aufgabe des Gesetzgebers und sodann durch die Empfehlungen und Entscheidpraxis des EDÖB's zu erreichen. Entsprechend lehnt der SDV alle vorgesehenen Instrumente des Entwurfes ab, mit dem der Zugang zu zivilrechtlichen Verfahren für die klagenden Parteien über eine Abschaffung von Verfahrenskosten vereinfacht werden sollen ab. In aller Regel sind es nicht die gesetzlich vorgesehenen Gerichtskosten und damit zusammenhängenden zivilprozessualen Voraussetzungen, die in Bezug auf den Entscheid, eine Klage zu erheben, abschreckend wirken.
SDV	ZPO	113	2	g	Der SDV lehnt die Befreiung von Gerichtskosten in zivilrechtlichen Verfahren zur Durchsetzung des Datenschutzgesetzes (Verfahren nach Art. 25 VE-DSG) ab.
SDV	ZPO	114		F	Der SDV lehnt die Befreiung von Gerichtskosten in zivilrechtlichen Verfahren zur Durchsetzung des Datenschutzgesetzes (Verfahren nach Art. 25 VE-DSG) ab.

Erläuternder Bericht Kapitel 8 "Erläuterungen zu den einzelnen Artikeln"

Name/Firma	Art.	Bemerkung/Anregung
SDV	3 lit. a	Die **Ausführungen zum Begriff der Personendaten sind unklar und potentiell widersprüchlich**. Auf der einen Seite soll der Begriff „Personendaten“ gemäss Bericht gegenüber dem geltenden Recht zwar inhaltlich nicht geändert werden. Dabei ist insbesondere die implizite Anerkennung der relativen Methode, wie sie auch in der EU künftig weiterhin gelten soll, zentral und richtig. Auf der andern Seite wird im Bericht jedoch eine natürliche Person als bestimmbar erklärt, wenn sie „über Hinweise auf eine Identifikationsnummer oder eine Online-Identität“ identifiziert werden kann. Diese Formulierung ist gerade in diesem für sämtliche Online-Aktivitäten fundamentalen Punkt missverständlich und je nach Interpretation widersprüchlich. Denn nach der wohl herrschenden Auffassung genügt es unter dem geltendem DSG nicht, wenn Angaben bloss einer bestimmten „eindeutigen Kennung“ oder „Identifikationsnummer“, wie z.B. einer IP-Adresse oder Cookie-Kennungen zugeordnet werden können, hinter welcher letztlich eine Person steht, diese aber nicht namentlich identifiziert werden kann (sog. Singularisierung). Bei der Qualifikation von IP-Adressen etc. muss daher auch künftig eine Einzelfallbeurteilung entscheidend sein, unter Berücksichtigung des Aufwands zur Identifizierung mit den zur Verfügung stehenden technischen Möglichkeiten (objektive Seite) sowie dem Interesse an der Identifizierung (subjektive Seite). Insbesondere beim Einsatz von Cookies zur Auslieferung von individualisierter Werbung auf Websites, bei welchem regelmässig auch die IP-Adresse mitbearbeitet wird, besteht kein Interesse an der namentlichen Identifikation des Nutzers, sondern lediglich an der Kategorisierung. Würde hier stets von Personendaten ausgegangen werden müssen, hätte dies erhebliche Auswirkungen auf die gesamten Online-Aktivitäten, sodass letzten Endes zahlreiche heute werbefinanzierte, unentgeltliche Angebote künftig nicht mehr allgemein zur Verfügung stehen würden. **Vor diesem Hintergrund ist eine Klarstellung in der Botschaft, dass das Konzept der Singularisierung abgelehnt wird, von zentraler Bedeutung**. Der Umstand, dass nach Auffassung einzelner Autoren unter der EU-DSGVO eine Singularisierung für das Vorliegen von Personendaten ausreichen soll, ändert daran nichts. Denn zum einen wird diese Auffassung von anderen Autoren mit überzeugenden Argumenten abgelehnt. Zum anderen ergibt sich eine derart strenge Auslegung auch nicht aus dem E-SEV 108, weshalb keine Notwendigkeit besteht, sie im Schweizer Recht einzuführen.
SDV	3 lit. f	Der **Begriff des Profiling** ist nach der vorgeschlagenen Regelung **untauglich und realitätsfremd**. Hier sind Konkretisierungen und Beispiele angezeigt, damit Klarheit herrscht, welche konkreten Tätigkeiten als Profiling zu betrachten sind.

SDV	4 Abs. 6	**Die vorgeschlagene Änderung hinsichtlich des Begriffs der „Einwilligung“ ist unter Einbezug des erläuternden Begriffs unklar**. Gemäss erläuterndem Bericht (S. 47) ermöglicht die Neuformulierung eine terminologische Annäherung an die DSGVO. Es wird allerdings nicht klargestellt, ob damit eine inhaltliche Annäherung bezweckt wird. **Die Definition ist nicht nur, aber in besonders ausgeprägter Form gerade für die Werbebranche von fundamentaler Bedeutung, weshalb eine klare Regelung und damit Rechtssicherheit erforderlich ist.** Die Übernahme der Vorgaben der EU-DSGVO in Bezug auf die „Freiwilligkeit der Einwilligung“ (Art. 7 Abs. 4) hätte jedenfalls eine massive Verschärfung der Rechtslage gegenüber dem geltenden Recht sowie eine erhebliche Beschränkung der Vertragsfreiheit zur Folge, die unnötig und daher abzulehnen ist. **Der E-SEV 108 (Art. 5 Abs. 2) verlangt denn auch lediglich, dass die Einwilligung freiwillig sein muss („free consent“), ohne eine derart strenge Interpretation, wie sie die EU-DSGVO enthält, vorzuschreiben.** In der Botschaft muss deshalb eine entsprechende Klarstellung aufgenommen werden. Darüber hinaus sind die Ausführungen im erläuternden Bericht zur „ausdrücklichen Einwilligungen“ unklar bzw. unvollständig. Es geht daraus letztlich nicht hervor, welche Anforderungen konkret an eine solche Einwilligung gestellt werden, was gerade aufgrund des (noch) übermässig weit gefassten Begriffs des Profiling und dessen Bedeutung für die Werbebranche besonders problematisch ist. **Es ist daher in der Botschaft auch klar zu stellen, dass – wie nach geltendem Recht – eine Einwilligung dann ausdrücklich ist, wenn die Datenbearbeitung, in welche eingewilligt wird, also z.B. das Profiling bspw. in der Datenschutzerklärung beim Namen genannt wird und es insofern nicht genügen würde, wenn bloss aus den Umständen auf ein Profiling geschlossen werden müsste**. **Schliesslich ist in der Botschaft auch festzulegen, dass – entsprechend dem geltenden Recht – eine Einwilligung auch zu einem Dokument, das weitere Informationen erhält (wie z.B. AGB oder Datenschutzerklärungen), erteilt werden kann und keine separate Information bzw. Einwilligung erforderlich ist.**
SDV	8	**Es muss zumindest in der Botschaft klargestellt werden, wer zu den interessierten Kreisen gehört**. So sollte insbesondere eine Mitwirkung von Konsumentenverbänden ausgeschlossen werden, da deren Interessen bereits durch den Genehmigungsvorbehalt des EDÖB ausreichend berücksichtigt werden. **Sodann ist ein Rechtsmittel gegen die Genehmigungsentscheide vorzusehen.** Zur Klärung der Rechtslage in Bezug auf die Rechtsmittel (insb. Legitimation) gegen einen Entscheid über die Genehmigung von Empfehlungen sind hier zumindest Erläuterungen in der Botschaft angezeigt. Die Rechtsmittel, welche allgemein auch im E-SEV 108 verlangt werden (Art. 12bis Abs. 6), sind umso mehr von Bedeutung, als aufgrund der Pflicht zur Genehmigung durch den EDÖB zu erwarten ist, dass mit den Empfehlungen ein über die gesetzlichen Vorgaben hinausgehender Standard gesetzt wird. Dieser wird letztlich auch trotz der expliziten Regelung in Art. 9 Abs. 2 VE-DSG faktisch zum Gesetz werden. Folglich muss eine klare Regelung bestehen, die es den betroffenen Verbänden bzw. Unternehmen ermöglicht, die Nicht-Genehmigung bzw.

		Ablehnung einer Empfehlung, die den gesetzlichen Vorgaben entspricht, gerichtlich anzufechten.
SDV	13	Nach der vorgeschlagenen Regelung ist unklar, inwiefern die Informationspflicht auch gilt, wenn nachträglich neue Bearbeitungszwecke hinzukommen oder andere Bearbeitungen an die Stelle der ursprünglichen treten. Diesbezüglich ist zumindest in der Botschaft eine Klarstellung erforderlich, dass nur über das informiert werden muss, was schon zum Zeitpunkt der Beschaffung feststand. Denn in solchen Fällen wäre in der Regel ohnehin eine Einwilligung oder ein anderer Rechtfertigungsgrund erforderlich und eine Sanktionsbewehrung folglich unverhältnismässig. Zudem müsste klargestellt werden, dass – entsprechend der geltenden Rechtslage und der Praxis des EDÖB – bei der Beschaffung grundsätzlich ein Verweis auf die auf der Website enthaltenen Detailinformationen ausreicht. Die Erwägung im erläuternden Bericht, wonach es nicht genügt, wenn die betroffene Person nach den Informationen suchen muss, sollte deshalb zumindest im Rahmen der Botschaft in diesem Sinne präzisiert werden. Hinsichtlich des Zeitpunkts der Information ist für den Online-Kontext eine Klarstellung erforderlich. Denn beim Zugriff auf eine Website wird regelmässig eine Bearbeitung von IP-Adressen erfolgen (Erfassung in Log-Datei, Zählung der Website-Zugriffe etc.) und dies in der Regel bereits bevor der Nutzer allfällige Informationen hierzu z.B. in einer Datenschutzerklärung zur Kenntnis nehmen kann. Aufgrund der Tatsache, dass IP-Adressen je nach Einzelfall Personendaten darstellen können und dass eine vorgängige Information hier technisch grundsätzlich nicht möglich ist, muss klargestellt werden, dass die ausreichend kenntlich gemachte Information in einer Datenschutzerklärung nach Abruf der Website als rechtzeitig gilt.
SDV	15	Hier muss klargestellt werden, dass auch „rechtliche Auswirkungen“ eine gewisse Schwere aufweisen müssen.
SDV	18	Hier muss den Datenbearbeitern im Sinne der „Business Judgement Rule“ ein gewisser Ermessensspielraum eingeräumt werden. In der Botschaft ist dies klarzustellen.
SDV	23 Abs. 3	Die Erwägung im erläuternden Bericht, wonach die Regelung nur zum Tragen komme, wenn die Bearbeitung dieser Daten auch rechtmässig erfolgt (S. 69), ist unzutreffend und daher in der Botschaft klar zu stellen.
Fehler! Verweisquelle konnte nicht gefunden werden.	24 Abs. 2	Der SDV fordert sodann, dass entsprechend der EU-DSGVO (Erw.-Gr. 47) zumindest in der Botschaft darauf hinzuweisen ist, dass die Bearbeitung von Personendaten zum Zwecke der Direktwerbung ein überwiegendes Interesse darstellen kann.
Fehler! Verweisquelle	50 ff	**Das vorgeschlagene Sanktionssystem, das primär auf die persönliche strafrechtliche Verurteilung von natürlichen**

konnte nicht gefunden werden.		**Personen abstellt, wird strikt abgelehnt**. Dieses vorgesehene Sanktionssystem steht der Digitalen Strategie der Schweiz diametral entgegen. Es ist in höchstem Mass innovationshemmend und etabliert eine Kultur des Denunziantentums in den Unternehmen. Es führt zu einem ganz erheblichen Standortnachteil der Schweiz. Kein innovatives digitales Start-Up wird bereit sein, seine Gründer und Mitarbeiter solch drastischen strafrechtlichen Risiken auszusetzen. Gute Mitarbeiter werden nicht mehr bereit sein Verantwortung in den Unternehmen mitzutragen. Insbesondere aufgrund der vorgesehenen Strafbarkeit fahrlässigen Verhaltens wird potentiell jeder Mitarbeiter durch heute alltägliche Verrichtungen am Arbeitsplatz ständig Gefahr laufen, sich strafbar zu machen. Dies ist auch gesellschaftspolitisch komplett inakzeptabel. Gleichzeitig ist es gegenüber Datenbearbeitungen durch ausländische Unternehmen faktisch nicht durchsetzbar, was sodann einerseits den Datenschutz in der Schweiz nicht erhöht und andererseits ausländischen Unternehmen einen immensen Wettbewerbsvorteil verschafft. Sodann würde die Schweiz damit gegenüber der EU in diesem grundlegenden Punkt einen Sonderweg einschlagen. Selbst wenn gemäss dem E-SEV 108 nicht zwingend administrative Bussen verlangt werden, wird gleichwohl eine unnötige Unsicherheit im Hinblick auf die Beurteilung der Angemessenheit des Schweizer Datenschutzrechts geschaffen. Ferner wird die Abweichung wie erwähnt international aber auch schon im europäischen Kontext zu vollstreckungsrechtlichen Schwierigkeiten führen (Stichwort: Voraussetzung der doppelten Strafbarkeit), was letztlich zu einer Bevorzugung von ausländischen Unternehmen gegenüber den einheimischen führt. **In jedem Falle wird die vorgeschlagene Regelung aber auch die für die Schweizer Wirtschaft zentralen Verhandlungen zwischen der Schweiz und der EU über die Koordinierung der Anwendung des jeweiligen Datenschutzrechts und die Abgrenzung der Zuständigkeit der Aufsichtsbehörden (Motion Fiala, 16.3752) erheblich erschweren.** Es erscheint gänzlich unrealistisch, dass die EU eine entsprechende Vereinbarung abschliesst, wenn in der Schweiz Unternehmen, die Datenschutzverletzungen gegenüber EU-Bürgern begehen, nur in Ausnahmefällen bzw. nach Ermessen der Untersuchungsbehörden verfolgt werden können. Darüber hinaus greift auch die Begründung „mit Blick auf die Kosten“ im erläuternden Bericht viel zu kurz. Die Kosten werden mit der vorgeschlagenen Regelung lediglich auf die kantonalen Strafbehörden übertragen. Es ist nicht ersichtlich, inwiefern sich diese hierdurch verringern sollten. Im Gegenteil ist ein solches **System ineffizient und wird gesamtwirtschaftlich deutlich höhere Kosten verursachen**, da neben dem Verwaltungsverfahren des EDÖB bei Verdacht auf strafrechtlich relevante Verhaltensweisen ein zusätzliches Strafverfahren mit neuerlichen Untersuchungsmassnahmen durchzuführen ist. Der gleiche Fall müsste folglich zweimal untersucht werden. Dies würde auch für die Unternehmen zu einem nicht vertretbaren und unnötigen Mehraufwand führen. **Schliesslich ist auch die primäre strafrechtliche Sanktionierung der natürlichen Personen an sich unverhältnismässig und**

		mit Blick auf den Datenschutz nicht zielführend. Die betroffenen Mitarbeiter würden durch das Risiko einer strafrechtlichen Verurteilung massiv unter Druck gesetzt. Namentlich bei Kenntnis einer Verletzung müssten sie entweder den zuständigen Mitarbeiter denunzieren oder würden sich andernfalls unter Umständen gar selbst strafbar machen. Ferner besteht die Gefahr, dass Unternehmen nach Möglichkeit einen unliebsamen Mitarbeiter im Sinne eines „Bauernopfers“ für den massgeblichen Verstoss als zuständig bezeichnen und sich so letztlich aus der Verantwortung nehmen können. **Zudem würde gerade die Position von betrieblichen Datenschutzverantwortlichen, die eigentlich zur Erhöhung des Datenschutzes beitragen sollten, mit dem vorgeschlagenen System erheblich geschwächt.** Statt der Förderung des betrieblichen Datenschutzes würde damit eine Kultur der Verschleierung geschaffen. Insbesondere in kleineren Unternehmen, in welchen die zuständige Person einfacher ausfindig zu machen ist, dürfte kaum mehr jemand bereit sein, eine entsprechende Stelle, resp. die entsprechende Verantwortung zu übernehmen. **Geradezu absurd erscheint die Schärfe des vorgeschlagenen Sanktionssystems, wenn man bedenkt, dass damit ausgerechnet der materielle Kern eines wirksamen Datenschutzes, nämlich die Beachtung der Bearbeitungsgrundsätze, nicht sanktionsbedroht sein soll**. Dies im Übrigen natürlich zu Recht. Spätestens in diesem Zusammenhang wird nämlich klar, dass sich das Strafrecht als disziplinierendes Instrument in diesem Bereich nicht eignet. In einem Rechtsstaat kann ein Verhalten nur strafbar sein, wenn der zugrundeliegende Tatbestand eindeutig bestimmt ist. Gerade dies ist aber im Bereich des Datenschutzes in den meisten Fällen nicht der Fall: wie soll ein Mitarbeiter voraussehen können, ob die mit einer Bearbeitung verbundenen Risiken genügend „erhöht“ sind, um damit die strafrechtlich sanktionierte Pflicht einer Risiko-Folgenabschätzung im Sinne von Art. 16 VE-DSG auszulösen? **Vor diesem Hintergrund sind anstelle von Strafsanktionen verwaltungsrechtliche Bussen einzuführen.** Für Binnensachverhalte ist es allerdings nicht angezeigt, die Bussenrahmen der EU-DSGVO zu übernehmen. Hier genügen tiefere Maximalsanktionen. Mit Blick auf eine allfällige Koordinations-Vereinbarung mit der EU sollten die Obergrenzen für Verstösse, die den EU-Markt betreffen, allerdings höher ausfallen. Der SDV schliesst sich der Forderung der economiesuisse nach einem Sanktionssystem entsprechend den folgenden Grundsätzen an: Die Sanktionen sollen sich primär an die Unternehmen richten und verwaltungsrechtlicher Natur sein. Eine Sanktionierung von Mitarbeitenden ist nur für Fälle von direkt vorsätzlichen Verstössen vorzusehen, in welchen sich das Handeln des Mitarbeiters gegen die Interessen des Unternehmens oder der betroffenen Person richtet. Der Kreis der potentiell verantwortlichen Mitarbeitenden muss dabei klar definiert und angemessen eingeschränkt werden.

		Des Weiteren ist der Strafkatalog anzupassen. Dieser darf in keinem Fall über die EU-DSGVO hinausgehen. Zu offen formulierte Tatbestände sind dabei entweder aus dem Katalog zu entfernen oder zu konkretisieren. Zudem ist eine Erheblichkeitsschwelle einzuführen, die sich an der Schwere der Persönlichkeitsverletzung oder an der Höhe des entstandenen Schadens orientiert. Auf die Sanktionierung von fahrlässig begangenen Verstössen ist zu verzichten. Schliesslich ist auch kooperatives Verhalten durch geeignete Anreize zu fördern, indem Sanktionen bei Vorliegen von schadensminderndem Verhalten wegfallen oder zumindest reduziert werden. Im Übrigen verweisen wir auf die ausführliche Stellungnahme der economiesuisse in deren Vernehmlassungsantwort.
Fehler! Verweisquelle konnte nicht gefunden werden.	Seite 64	Datenschutzfreundliche Voreinstellungen 1. Wir sind nicht einverstanden mit der Feststellung, dass das Anlegen eines Benutzerkontos schon zu einer umfassenderen Bearbeitung von Personendaten führt. Jede Online-Bestellung führt zu einem Zusammenführen von Einkaufshistorie und Kunde, das Anlegen eines Benutzerkontos oder Benutzerprofils ist eine reine administrative Tätigkeit, welche nicht zwingend zu umfassenderen Daten führt! 2. Nicht eingegangen wird hier auf das Thema Cookies / Nachverfolgung von Kundenbewegungen.
Fehler! Verweisquelle konnte nicht gefunden werden.	Seite 88	Übergangsbestimmungen Die Übergangsbestimmungen müssen insbesondere für Altdaten ergänzt worden. Es ist ausdrücklich festzuhalten, dass Personendaten, die unter dem alten Recht rechtmässig erhoben und bearbeitet wurden, im entsprechenden Umfang auch unter dem neuen Recht weiterhin bearbeitet werden dürfen. Schlussendlich ist eine angemessene Übergangsfrist von mindestens zwei Jahren für die Umsetzung aller neuen Pflichten unter dem Gesetz vorzusehen um den Unternehmen die Umstellung ihrer Prozesse zu ermöglichen. Eine entsprechende Übergangsfrist hat auch die EU-DSGVO nach ihrem Inkrafttreten vorgesehen. Diese wird im Frühling 2018 auslaufen.