Per Email: digitaltest@seco.admin.ch

Staatssekretariat für Wirtschaft SECO
Direktion für Wirtschaftspolitik
Ressort Wachstum und Wettbewerbspolitik
Holzikofenweg 36
3003 Bern

Bern, 30. Juni 2017

„Digitaler Test" – Stellungnahme von ICTswitzerland

Sehr geehrte Damen und Herren

Wir beziehen uns auf Ihre E-Mail vom 3. April 2017 betreffend dem *Digitalen Test*, in welcher Sie uns um Rückmeldung zu bestehenden Hürden für die Digitalisierung beziehungsweise für digitale Geschäftsmodelle in der Schweiz gebeten haben. Wir möchten uns zunächst dafür bedanken, dass Sie ICTswitzerland Gelegenheit zu einer Stellungnahme geben und hoffen, Ihnen mit den nachfolgenden Ausführungen wertvolle Hinweise für die weitere Diskussion geben zu können.

ICTswitzerland ist der Dachverband der ICT-Wirtschaft. Der 1980 gegründete Verband umfasst 28 grosse und mittlere Unternehmen sowie 21 Verbände. ICTswitzerland vertritt deren Anliegen gegenüber der Öffentlichkeit, den Behörden und anderen Verbänden, bezweckt die Förderung und Weiterentwicklung der digitalen Technologien sowie die Aus- und Weiterbildung von ICT-Fachkräften. In der Schweiz werden in allen Wirtschaftsbranchen und in der öffentlichen Verwaltung 210'000 ICT-Fachkräfte beschäftigt (2015). Mit einer Bruttowertschöpfung von CHF 28 Mrd. (2014) ist die ICT-Kernbranche die sechstgrösste Wirtschaftsbranche der Schweiz.

ICTswitzerland hat in den vergangenen Wochen zahlreiche Leitfadengespräche sowie eine breite Umfrage bei seinen Mitgliederfirmen und Mitgliederverbänden durchgeführt. Die Rückmeldungen wurden von einer juristischen Expertengruppe ausgewertet und aufbereitet. Im Folgenden finden Sie die Ergebnisse unseres Digitalen Tests.

1 Allgemeine Überlegungen und Anregungen

Der heutige Gesetzgebungsprozess ist vom Versuch geprägt, neue Herausforderungen durch die Schaffung neuer Regularien zu meistern. Dies führt zu immer umfangreicheren Spezialgesetzgebungen und einer grossen Rechtszersplitterung. Die Folgen für kleinere und mittlere Unternehmen und speziell auch für Start-up-Unternehmen sind vermehrt höhere Aufwendungen im Zusammenhang mit der Bewältigung und Befolgung dieser Regularien und eine Vielzahl von sich überschneidenden Regularien in ein und demselben Rechtsbereich.

Wir sind daher überzeugt, dass nicht nur ein Abbau von unnötigen Regularien erfolgen muss, sondern auch im Gesetzgebungsprozess grössere Anstrengungen unternommen werden müssen, um der Regulierungsvielfalt und ausufernden Spezialgesetzgebungen Einhalt zu bieten. Ein wichtiger Beitrag hierfür kann z.B. dadurch geleistet werden, dass nicht für jede neue technologische Herausforderung ein neuer Erlass geschaffen wird, sondern bestehende Regularien und Rechtsinstitute genutzt und ggf. angepasst werden, damit sie auch auf aktuelle und künftige technische Entwicklungen und die Digitalisierung angewendet werden können. So kann z.B. der Problematik „booking.com“ durch Anwendung der bestehenden wettbewerbsrechtlichen Regeln Einhalt geboten werden, statt dafür wiederum neue Regulierungen und Hürden zu schaffen. Wichtig ist in diesem Zusammenhang auch, dass die Konsequenzen von neuen Regulierungen bedacht werden. So sind z.B. im revidierten Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (revBüPF) diverse neue Aufgaben für den Bund enthalten, wofür zusätzliches Personal notwendig sein wird. Jedoch hat das Parlament mit seinem Sparbeschluss entschieden, dass die Zahl der Bundesangestellten nicht wachsen darf, was die Umsetzung des revBüPF gefährdet.

2 Die konkreten Digitalisierungshürden in den einzelnen Regulierungsbereichen

Mit Blick auf konkrete Regulierungsbereiche, welche Hürden für die Digitalisierung und digitale Geschäftsmodelle und v.a. auch im Hinblick auf die digitale Transformation bilden , möchten wir folgende Rechtsbereiche herausgreifen und nachfolgend näher ausführen:

2.1 Herausgabe von Daten im Konkurs

2.1.1 Problematik

Der Konkursfall eines Cloud-Providers stellt Kunden und Nutzer heute vor grosse Probleme. Der Eigentümer von Daten, die er als Kunde eines Cloud-Providers bei einem solchen hinterlegt, hat keine Möglichkeit, diese wieder heraus zu verlangen, wenn der Cloud-Provider in Konkurs fällt. Dies einerseits, weil Computerdaten sachenrechtlich keine beweglichen Sachen darstellen. Anderseits fehlt es einer rechtlichen Grundlage, um bei einer Konkursverwaltung den Antrag auf Rückgabe der hinterlegten Daten zu stellen.

2.1.2 Wirkungen bei Wegfall des Hindernisses

Die heutige Gesetzeslage hat einschneidende Konsequenzen für den Dateneigentümer im Falle eines Konkurses eines Cloud-Providers, da auch vertragliche Regelungen in solchen Fällen keinen adäquaten Schutz

gewähren können. Sie schadet letztlich auch der Attraktivität von Cloud-Angeboten aus der Schweiz und damit der Weiterentwicklung des Wirtschaftsstandorts im Hinblick auf attraktive ICT-Dienstleistungen aus der Schweiz. Es ist daher nicht nur wünschenswert, sondern eine Notwendigkeit, dass sich der Gesetzgeber diesen kontraproduktiven Effekten eines Konkurses annimmt. Die in der parlamentarischen Initiative Dobler, Nr. 17.410, vorgeschlagene Anpassung von Art. 242 SchKG des BG über Schuldbetreibung und Konkurs (SchKG) schafft Rechtssicherheit und verhilft zu einer praxistauglichen Lösung.

2.2 Datenschutzgesetzgebung

2.2.1 Problematik

Am 21. Dezember 2016 präsentierte der Bundesrat den Vorentwurf für ein totalrevidiertes Datenschutzgesetz (VE-DSG). Datenschutz spielt in der ICT-Branche eine ganz zentrale Rolle. Die Unternehmen der ICT-Branche sind daher auf eine diesbezüglich praxisnahe und wirtschaftsfreundliche Regelung besonders angewiesen und daher von dieser Vernehmlassungsvorlage direkt betroffen.

ICTswitzerland ist überzeugt, dass die Schweiz einen wirksamen Datenschutz und die nötige Äquivalenz gegenüber den EU Standards mit einer – im Gegensatz zum Vorentwurf – schlanken Gesetzesrevision erreichen kann. Insbesondere ein «Swiss Finish», der über die internationalen Standards hinausgeht, ist schädlich und strikt zu vermeiden. Aus Sicht der ICT-Wirtschaft sind sodann vor allem folgende Anpassungsforderungen zentral:

- Die Informations- und Meldepflichten im VE-DSG gehen deutlich zu weit. Sie sind substantiell zu reduzieren. So sind insbesondere die überschiessenden Meldepflichten an den Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auf Verstösse mit gravierenden Folgen zu beschränken.
- Das Sanktionssystem im VE-DSG sieht strafrechtliche Sanktionen gegen Mitarbeitende von bis zu 500‘000 Franken vor. Dies ist weder verhältnismässig noch zielführend. Es sollen Verwaltungsstrafen gegen Unternehmen im Vordergrund stehen; wenn nicht vorsätzliches Handeln der Mitarbeitenden vorliegt. Ein Strafkatalog, der über die EU Standards hinausgeht, ist abzulehnen.
- Im Sinne der erfolgreichen Tradition der Schweiz wird mehr vernünftige Selbstregulierung durch die Unternehmen gefordert. So müssen Empfehlungen der guten Praxis zwingend von (Branchen-)Verbänden ausgehen und nicht vom EDÖB in Eigenregie. Zudem ist auf freiwilliger Basis ein betrieblicher Datenschutzbeauftragter mit entsprechenden Erleichterungen für Unternehmen in das Datenschutzgesetz einzuführen.
- Die Ausstattung des EDÖB mit Untersuchungs- und neu auch Verfügungskompetenzen ist heikel. Eine saubere Trennung der Kompetenzen ist angezeigt.

Für weitere Forderungen sowie konkrete Anpassungsvorschläge des VE-DSG verweisen wir auf die vollständige Stellungnahme des ICTswitzerland zum VE-DSG vom 4. April 2017, welche wir Ihnen als Anlage 1 zu diesem Schreiben zustellen.

2.2.2 Wirkungen bei Wegfall des Hindernisses:

Eine schlanke Revision des Datenschutzgesetzes, wie sie ICTswitzerland in seiner Stellungnahme zum VE-DSG vom 4. April 2017 fordert, führt zu einem wirksamen, den internationalen Standards genügenden Datenschutz, welcher aber auch ein Maximum an Flexibilität für den Schweizer Wirtschaftsstandort sichert, die Unternehmen vor unnötigem administrativem und finanziellen Aufwand bewahrt, und den Zugang zum internationalen Markt nicht unnötig einschränkt.

2.3 Arbeitsgesetzgebung

2.3.1 Problematik

Die Diskrepanz zwischen der Pflicht zur detaillierten Arbeitszeiterfassung und der Realität des Arbeitsalltags wird laufend grösser und die gesetzliche Pflicht sind schlicht nicht mehr zeitgemäss. Eine Lockerung der Aufzeichnungspflicht ist unabdingbare Voraussetzung für den modernen Arbeitsalltag und für einen digitalen Arbeitsplatz. Ein vollständiger Verzicht auf die Arbeitszeiterfassung ist leider auch nach der am 1.1.2016 in Kraft getretenen Verordnung 1 zum Arbeitsgesetz nur unter einem Gesamtarbeitsvertrag (GAV) und weiteren Voraussetzungen zulässig. Die geänderte Verordnung ermöglicht somit weiterhin nur unter sehr einschränkenden und restriktiven Bedingungen eine Flexibilisierung der Arbeitszeiterfassung und ist dann erst noch mit erheblichem administrativem Aufwand für Mitarbeiter und das Unternehmen verbunden.

2.3.2 Wirkungen bei Wegfall des Hindernisses

Mit der Einführung von weniger restriktiven Voraussetzungen für die erleichterte Arbeitszeiterfassung bzw. eines gänzlichen Wegfalls der Erfassungspflicht (und eine weitere Teilflexibilisierung des Arbeitsgesetzes, wie sie in der parlamentarischen Initiative Graber, Nr. 16414, verlangt wird) wird die Arbeitsgesetzgebung an die heutigen Gegebenheiten der Arbeitswelt und an die heute bereits gelebte Realität angepasst. Sie unterstützt zudem die Modernisierung der Arbeitszeitmodelle im Rahmen auch einer digitalen Arbeitswelt mit digitalem Arbeitsplatz.

2.4 Fachkräfte: Grössere Kontingente für Fachspezialisten

2.4.1 Problematik

Ende November 2014 hatte der Bundesrat beschlossen, die Kontingente für Kurzaufenthalter (L-Bewilligungen) ab 1. Januar 2015 massiv zu reduzieren. Dabei geht es um Aufenthalte von Arbeitskräften bis zu 12 Monaten (wobei Aufenthalte unter vier Monaten diesem Regime nicht unterstellt sind). Kurzaufenthalter sind meist erforderlich, um IT-Spezialisten, welche in der Schweiz nicht verfügbar sind, ins Land zu holen, die das lokale Projektteam vervollständigen. Ist dies nicht möglich, so wird das Projekt oft nicht in der Schweiz, sondern im Ausland abgewickelt, womit auch die Schweizer Team-Mitglieder den entsprechenden Projektauftrag verlieren. Die Wertschöpfung wandert aus der Schweiz ab. Die verfügbare Anzahl L-Kontingente ist trotz verschiedener Interventionen nach wie vor viel zu klein, um den Bedarf abdecken zu können. Die Auswirkungen haben die Mitglieder aus der ICT-Branche seither zu spüren bekommen. Seit der Kürzung für 2015 waren die Kontingente für die jeweiligen Quartale schon in etwa zur Halbzeit aufgebraucht, was dazu führt, dass „zu spät“ kommende Unternehmen leer ausgehen, und insgesamt eine hohe Unsicherheit z.B. bei der Offertstellung für internationale Projekte für ICT Unternehmen in der Schweiz besteht.

Eine ähnliche Problematik besteht auch im Bereiche der in der Schweiz an Hochschulen ausgebildeten ausländischen Fachkräfte aus Drittstaaten. Aufgrund von ausgeschöpften Kontingenten müssen diese nach Abschluss ihres Studiums oftmals die Schweiz verlassen, obwohl diese unmittelbar nach dem Abschluss des Studiums eine Stelle antreten könnten.

2.4.2 Wirkungen bei Wegfall des Hindernisses:

Eine Rückkehr zumindest zur Höhe der Kontingentszahlen aus dem Jahre 2014 (d.h. eine Verdoppelung der Drittstaatenkontingente und eine Verdreifachung der EU/EFTA Dienstleistungserbringer-Kontingente) fördert die Stellung der ICT-Unternehmen in der Schweiz und stärkt damit letztlich den Werkplatz Schweiz und die heimische ICT-Industrie.
Die in der Motion Dobler, Nr. 17.3067, vorgeschlagene Anpassung von Art. 21 der Verordnung über Zulassung, Aufenthalt und Erwerbstätigkeit (VZAE), nach welcher vorgenannte Fachkräfte nicht mehr den Kontingenten angerechnet würden, kann zudem einen wesentlichen Beitrag dazu leisten, dass gefragte Fachkräfte aus Drittstatten nach ihrem Studium in der Schweiz verbleiben und nicht ins Ausland abwandern müssen.

2.5 Einführung der Elektronischen Identität

2.5.1 Problematik

Die elektronische Identität ist eine Grundlage für viele digitale Anwendungen, seien dies private oder staatliche – vom Online-Shopping über E-Banking bis zum E-Voting. Wenn die Schweiz den Zug der Digitalisierung nicht verpassen will, ist es höchste Zeit, bei der Schweizer E-ID rasch voranzutreiben. E-IDs sind denn auch in anderen europäischen Ländern (z.B. Schweden, Lettland etc.) bereits im Einsatz.

2.5.2 Wirkungen bei Wegfall des Hindernisse

Im Rahmen der soeben abgeschlossenen Vernehmlassung zum E-ID-Gesetz unterstützt ICTswitzerland das Ziel des Bundes, die rechtlichen und organisatorischen Rahmenbedingungen zur Einführung einer elektronischen Identität für natürliche Personen zu schaffen. Jede Schweizerin und jeder Schweizer könnte sich damit im Internet mit der gleichen Qualität elektronisch ausweisen, wie mit dem Pass oder der Identitätskarte in der physischen Welt.

2.6 Förderung von Start-up-Unternehmen

2.6.1 Problematik

Die Schweiz scheint gute Voraussetzungen für Start-up-Unternehmen zu bieten: innovative Köpfe, politische Stabilität und kontinuierliches Wirtschaftswachstum. Und doch hat sich die Schweiz bisher keinen Namen als Start-up-Land gemacht. Einer der Gründe sind die heute vielerorts geltenden Steuergesetze, wonach Aktien der Start-up-Unternehmen nach Preisen der letzten Finanzierungsrunde bewertet werden. Dies führt gerade bei investitionslastigen Start-up-Unternehmen zu hohen Steuerrechnungen, die in der Wachstumsphase nicht beglichen werden können. Die Konsequenz ist deshalb die, dass rasch wachsende Unternehmen tendenziell ihren Sitz ins Ausland verlegen.[1]

[1] Siehe dazu :EPFL - College of Management of Technology, Switzerland's Digital Future, S. 34; abrufbar unter: six-group.com/digitalch or swisscom.ch/digitalch.

2.6.2 Wirkungen bei Wegfall des Hindernisses

Eine Entlastung bei der Besteuerung von Start-up-Unternehmen kann zur Etablierung einer Start-up-Kultur in der Schweiz beitragen und damit die Innovationskraft der ICT-Branche und des schweizerischen Wirtschaftsstandorts fördern. So hat beispielsweise der Kanton Zürich als Sofortmassnahme bereits im März 2016 beschlossen, Jungunternehmen in den ersten drei bis fünf Jahren nach ihrer Gründung nur zum bedeutend tieferen Substanzwert zu besteuern, und nicht danach, wie viel Geld sie durch Investoren erhalten haben.[2] In diesem Zusammenhang sind auch die neuesten Vorstösse im Parlament zu erwähnen, namentlich die Parlamentarische Initiative Nr. 17.456 betr. "Steuerliche Belastung aufgrund von Mitarbeiterbeteiligungen bei Start-ups und Familienunternehmen deutlich reduzieren" von Ruedi Noser (FDP/ZH), die Motion Nr. 17.3578 betr. „Ein attraktiver Forschungsplatz dank Start-up-Visa für Gründer" von Martin Bäumle (GLP/ZH) sowie die Motion Nr. 17.3580 betr. „Fairness für Start-Up-Unternehmen und KMUs bei der Arbeitslosenversicherung" von Jürg Grossen (GLP/BE), die es zu fördern gilt. Deren Umsetzung schafft die Voraussetzungen für eine erfolgreiche Start-up Unternehmenskultur in der Schweiz.

2.7 Verhinderung von Netzsperren

2.7.1 Problematik

Im Rahmen der noch laufenden Revision des Geld- und Glückspielrechts wurde im März 2017 vom Parlament beschlossen, in einem neuen Art. 84 des Bundesgesetzes über Geldspiele (revBGS) sogenannte „Netzsperren" einzuführen. Im Wesentlichen würden hierbei Anbieter von Fernmeldediensten verpflichtet, den Zugang zu ausländischen Online-Spieleveranstaltern über das Internet für in der Schweiz ansässige Nutzer zu unterbinden.

Fraglich ist dabei einerseits einmal generelle die technische Wirksamkeit solcher Netzsperren, da davon auszugehen ist, dass solche Sperren mit sehr wenig technischem Aufwand von interessierten Kreisen umgangen werden können. Überdies - und das ist unseres Erachtens schon im Ansatz kritisch – wird mit solchen staatlich eingeführten, untauglichen Netzsperren eine verfassungsmässig fragwürdige Einschränkung des digitalen Angebots verfügt, deren technische Umsetzung und damit zusammenhängende Aufwände zudem auch noch die Provider von Internetdienstleistungen zu tragen haben.

2.7.2 Wirkung bei Wegfall des Hindernisses

Wir halten eine Einführung von Netzsperren, wie sie im Rahmen des revBGS nun vorgesehen ist, deshalb für kritisch, weil sie als Basis dafür dienen könnte, in anderen von politischen Interessengruppen bearbeiteten Partikularinteressen eine untaugliche Zensurierung von Teilen des Internetangebots einzuführen, was letztlich im Widerspruch zu den Bestrebungen der länderübergreifend stattfindenden Digitalisierung und eines freiheitlichen Rechts- und Wirtschaftssystems steht. Damit wird auch die Wettbewerbsfähigkeit der Schweiz eingeschränkt.

[2] NZZ vom 1.11.2016: Zürich schafft bessere Bedingungen für Startups.

2.8 Ausbau der Mobilfunkinfrastruktur (USG und NISV)

2.8.1 Problematik

Bewilligungsverfahren, die im Umweltschutzgesetz (USG) geforderten vorsorglichen Schutzmassnahmen, die diesbezüglichen Konkretisierungen in der Verordnung über den Schutz vor nichtionisierender Strahlung (NISV) und raumplanerische Instrumente verzögern und verteuern den erforderlichen Ausbau der Mobilfunkinfrastruktur. Die Bewilligung von neuen Mobilfunkanlagen oder von Anlageänderungen erfolgt im kommunalen Baubewilligungsverfahren, wobei gleichzeitig auch stets die Einhaltung der NISV überprüft wird. Darin hat der Bundesrat gegenüber den meisten europäischen Ländern zehnfach strengere Grenzwerte und einschränkende Beurteilungsmethoden festgelegt (z.B. Hochrechnungen anstelle effektiver Belastungen). Leistungserhöhungen, Antennenwechsel oder Verwendung zusätzlicher Frequenzbänder müssen den Behörden gemeldet werden, was in der Regel eine erneute Baubewilligung zur Folge hat.

2.8.2 Wirkungen bei Wegfall des Hindernisse

Eine Harmonisierung der NISV-Anlagegrenzwerte auf 6 V/m, unabhängig der genutzten Frequenz, brächte mindestens kurzfristig bereits verfahrenstechnische Vereinfachungen und Erleichterungen. Weitergehende erforderliche Massnahmen in diesem Regulierungsbereich haben wir Ihnen in Anlage 2 dieser Stellungnahme zusammengefasst.

2.9 Anpassung des Fernmeldegesetzes (FMG) mit Ausführungsbestimmungen

2.9.1 Problematik: Art. 35 FMG

Die Eigentümerinnen und Eigentümer von Boden im Gemeingebrauch (wie Strassen, Fusswege, öffentliche Plätze, Flüsse, Seen sowie Ufer) sind verpflichtet, den Anbieterinnen von Fernmeldediensten die Benutzung dieses Bodens für Bau und Betrieb von Leitungen und öffentlichen Sprechstellen zu bewilligen, sofern diese Einrichtungen den Gemeingebrauch nicht beeinträchtigen. Die öffentlichen Sprechstellen gehören mittlerweile der Vergangenheit an und werden zurückgebaut. Demgegenüber entstehen neue Technologien wie Manhole Antennen, die in einem Schacht eingebaut werden, die aber nicht unter den Begriff Werkleitungen subsumiert werden können, da sie einen Teil des Mobilfunknetzes darstellen. Um den immer stärker wachsenden Datenvolumen zu begegnen, sind die Fernmeldedienstanbieter darauf angewiesen, die Mobilfunknetze laufend auszubauen, was einerseits mit Kosten verbunden ist und andererseits aufgrund der engen Umschreibung von Art. 35 FMG kantonale oder kommunale Rechte berücksichtigt werden müssen, was den Netzausbau erschwert.

2.9.2 Wirkungen bei Wegfall des Hindernisses: Art. 35 FMG

Eine Umschreibung im FMG, wonach der Boden im Gemeingebrauch entschädigungslos für Telekommunikationsanlagen benutzt werden kann, soweit der Gemeingebrauch nicht beeinträchtigt wird, würde den Rollout von neuen Telekommunikationsanlagen, welcher Art sie auch in Zukunft sein mögen, vereinfachen und sich positiv auf die Kosten auswirken.

2.9.3 Problematik: Art. 3 FMG

Vor dem Hintergrund der zunehmenden Bedeutung und Verbreitung von Internet of Things (IoT)- und Machine-to-Machine (M2M) Anwendungen stellt sich die Frage der Qualifikation von "klassischer M2M-Kommunikation" (automatisierter Informationsaustausch zwischen Endgeräten wie Maschinen, Automaten, Fahrzeugen, etc. untereinander oder mit einer zentralen Leitstelle ohne bzw. mit stark eingeschränkter menschlicher Interaktion) als Fernmeldedienst und der damit verbundenen Anwendbarkeit der für Fernmeldedienste geltenden regulatorischen Vorgaben. Wünschenswert wäre - analog dem deutschen Recht, welches zwischen Telekommunikationsdiensten und telekommunikationsgestützten Diensten unterscheidet - eine sachgerechte eingeschränkte Anwendbarkeit der regulatorischen Vorgaben auf "klassische M2M-Kommunikation.

2.9.4 Wirkungen bei Wegfall des Hindernisses: Art. 3 FMG

Die M2M Kommunikation ist nicht mit einem "üblichen" Telekommunikationsdienst zu vergleichen. M2M ist eine reine Datenübertragung zwischen Geräten, meist mit einem weitaus geringeren Übertragungsvolumen. Es ist nicht sachgerecht und hindert die Entwicklung des M2M Bereichs erheblich, wenn für diesen die gleichen Spielregeln angewendet werden, wir für einen herkömmlichen Telekommunikationsdienst.

2.9.5 Problematik: Art. 4 Abs. 3 lit. c und 11 Abs. 1 lit. c AEFV

Die durch das BAKOM zugeteilten Adressierungselemente (Rufnummern) müssen hauptsächlich für die Verwendung in der Schweiz vorgesehen sein, andernfalls das BAKOM die Zuteilung der Adressierungselemente verweigern kann (Art. 4 Abs. 3 lit. c Verordnung über die Adressierungselemente im Fernmeldebereich, AEFV). Falls bereits zugeteilte Adressierungselemente nicht mehr oder nicht hauptsächlich in der Schweiz verwendet werden, kann das BAKOM deren Zuteilung widerrufen (Art. 11 Abs. 1 lit. c AEFV). Die konkrete Bedeutung und Auslegung des Kriteriums der "hauptsächlichen Verwendung von Adressierungselementen in der Schweiz" ist unklar. Insbesondere stellt sich die Frage, ob sich die aus den vorgenannten Normen ergebende Einschränkung auf a) die gesamten, einer FDA zugeteilten Rufnummern, b) die einer FDA spezifisch zugeteilten Rufnummernbereiche, c) die jeweils zugeteilten Rufnummernblöcke, d) die jeweils im Rahmen eines konkreten Projektes/Vorhabens für einen Kunden eingesetzten Rufnummern oder sogar e) auf jede einzelne Rufnummer bezieht.

2.9.6 Wirkungen bei Wegfall des Hindernisses: Art. 4 Abs. 3 lit. c und 11 Abs. 1 lit. c AEFV

Vor dem Hintergrund der zunehmenden Bedeutung und Verbreitung von Internet of Things (IoT)- und Machine-to-Machine (M2M)-Anwendungen und der Tatsache, dass ein grenzüberschreitender Einsatz solcher Anwendungen in vielen Fällen ein Kundenbedürfnis darstellt, wäre eine Präzisierung der vorgenannten Normen dringend notwendig.

2.10 revBüPF und E-VüPF

2.10.1 Problematik: Art. 21/23 revBüPF i.V.m. Art. 19 E-VüPF

Diese demnächst in Kraft tretenden Bestimmungen des revidieren Bundesgesetztes betreffend die Überwachung des Post- und Fernmeldeverkehrs (revBüPF) bauen einerseits die von den Anbietern zu erfassenden Kundendaten aus (Art. 21 revBüPF) und geben andererseits dem Bundesrat die Kompetenz

festzulegen, wie diese Daten zu erfassen sind (Art. 23 revBüPF). Der Bundesrat kann demnach auf Verordnungsstufe massiv in die Vertragsabschlussmodalitäten eingreifen, was schon während des Gesetzgebungsverfahrens bemängelt wurde.

Die damals geäusserten Befürchtungen werden nun durch Art. 19 der Verordnung zum revBüPf (E-VüPF) leider bestätigt. Gemäss dieser Bestimmung könnte künftig ein Vertragsabschluss zu einem Fernmeldedienst generell (d.h. neu auch bei Festnetz- und Mobile-Abonnenten) nur noch nach persönlicher Identifikation des Kunden anhand eines vorgelegten gültigen amtlichen Ausweises und unter Anfertigung einer entsprechenden Ausweiskopie erfolgen. Diese Vorgabe würde den Vertrieb massiv beschränken und den reinen Online Abschluss von solchen Verträgen sogar verunmöglichen.

2.10.2 Wirkungen bei Wegfall des Hindernisses: Art. 21/23 revBüPF i.V.m. Art. 19 E-VüPF
Art. 19 E-VÜPF ist noch nicht in Kraft getreten. Insofern kann eine entsprechende Anpassung der Bestimmung das Eintreten der beschriebenen Nachteile verhindern.

2.10.3 Problematik: Art. 25 revBüPF i.V.m. Art. 29 Abs. 3 E-VüPF
Sowie Art. 25 revBÜPF in Art. 29 Abs. 3 E-VüPF umgesetzt werden soll, können neuartige Telekommunikationsdienstleistungen erst lanciert werden, wenn ihre Überwachungsfähigkeit gewährleistet, durch eine Bundesstelle (Dienst ÜPF) geprüft und bestätigt worden ist. Andernfalls können die Strafbestimmungen des revBÜPF greifen.

Diese Bestimmungen gehen von der - angesichts der rasanten technischen Entwicklung - unrealistischen Annahme aus, dass jeder Fernmeldedienst jederzeit überwachbar ist bzw. sein muss und es keine Lücken bei der Überwachung geben darf. Diese Überwachungsfähigkeit muss jetzt neu schon bei Markteinführung sichergestellt sein. Diese Bestimmungen sind offensichtlich innovationshemmend.

2.10.4 Wirkungen bei Wegfall des Hindernisses: Art. 25 revBüPF i.V.m. Art. 29 Abs. 3 E-VüPF
Art. 29 Abs. 3 E-VÜPF ist noch nicht in Kraft getreten. Insofern kann eine entsprechende Anpassung der Bestimmung das Eintreten der beschriebenen Nachteile verhindern.

3 Zusammenfassung

Die vorliegende Stellungnahme kann wie folgt zusammengefasst werden:

- Nicht nur ein Abbau von unnötigen Regularien ist anzustreben, sondern im Gesetzgebungsprozess müssen auch grössere Anstrengungen unternommen werden, um der Regulierungsvielfalt und ausufernden Spezialgesetzgebungen Einhalt zu bieten. Ein wichtiger Beitrag hierfür kann z.B. dadurch geleistet werden, dass nicht für jede neue technologische Herausforderung ein neuer Erlass geschaffen wird, sondern bestehende Regularien und Rechtsinstitute genutzt und ggf. angepasst werden, damit sie auch auf aktuelle und künftige technische Entwicklungen und die Digitalisierung angewendet werden können.

- Im Sinne einer Bekräftigung sind zudem die oben erwähnten Regulierungshürden anzugehen, und zwar in folgenden Bereichen:
  - Herausgabe von Daten im Konkurs (Ziffer 2.1)
  - Datenschutzgesetzgebung (Ziffer 2.2)
  - Arbeitsgesetzgebung (Ziffer 2.3)
  - Fachkräfte: Grössere Kontingente für Fachspezialisten (Ziffer 2.4)
  - Einführung der Elektronischen Identität (Ziffer 2.5)
  - Förderung von Start-up-Unternehmen (Ziffer 2.6)
  - Verhinderung von Netzsperren (Ziffer 2.7)
  - Ausbau der Mobilfunkinfrastruktur (Ziffer 2.8)
  - Anpassung des Fernmeldegesetzes (FMG) mit Ausführungsbestimmungen (Ziffer 2.9)

4 Schlussbemerkungen

Die Digitalisierung wird immer stärker zur treibenden Kraft für Innovationen in Wirtschaft und Gesellschaft. Die Chancen dieser Transformation proaktiv zu ergreifen, ist wesentlich, um die Schweiz auch zukünftig als innovativen und wettbewerbsfähigen Wirtschaftsstandort zu positionieren.

Um dieses Ziel zu erreichen bitten wir Sie um Berücksichtigung der oben ausgeführten Anliegen von ICTswitzerland.

Da es sich dabei um eine Momentaufnahme handelt, würde wir es überdies begrüssen, wenn ein Gefäss für eine regelmässige Überprüfung der Rahmenbedingungen für die digitale Wirtschaft geschaffen würde, und so sichergestellt werden kann, dass der Digitale Test nicht eine einmalige Aktion bleiben wird. Hierbei kann die Plattform „digital.swiss“, welche 2016 von ICTswitzerland ins Leben gerufen wurde und heute ein gemeinsames Projekt von ICTswitzerland, economiesuisse und digitalswitzerland ist, eine wichtige Basis bilden. Auf dieser Plattform beobachten Experten die Entwicklung zur Digitalisierung laufend und analysieren und diskutieren das Handlungspotenzial.

Wir danken Ihnen für Ihre Kenntnisnahme.

Freundliche Grüsse

Andreas Kaelin
Geschäftsführer

Anlage 1: ICTswitzerland Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG), 4.4.2017

Siehe separates PDF.

Anlage 2: Massnahmen im Regulierungsbereich «Ausbau der Mobilfunkanlagen»

Folgende Anpassungen der Regulierungen sind vorzunehmen:

- Eine Harmonisierung der NISV-Anlagegrenzwerte auf 6 V/m, unabhängig der genutzten Frequenz, brächte mindestens kurzfristig bereits verfahrenstechnische Vereinfachungen und Erleichterungen.
- Die Einführung einer neuen Anlagen-Kategorie in der NISV von beispielsweise 50 W ERP für Small Cells (mit erleichterten Anforderungen an NIS-Berechnungen) würde für Mobilfunkbetreiber eine Vereinfachung darstellen.
- Sämtliche Änderungen an Anlagen unterhalb des Anlagegrenzwertes sollten bewilligungsfrei vorgenommen werden können. In diesem Zusammenhang ist wichtig zu wissen, dass heute alle Anpassungen, welche in der NISV als Anlageänderungen deklariert sind, jedoch weiterhin im Rahmen der geltenden Grenzwerte erfolgen, neu bewilligt werden müssen.
- Im Weiteren sollten realistischere Beurteilungen der Exposition durch die Berücksichtigung des zeitlichen Mittelwertes in der Expositionsberechnung erfolgen und räumliche Mittelwertmessungen zur realitätsnahen messtechnischen Bewertung der Exposition und verbesserter Reproduzierbarkeit der Messresultate durchgeführt werden.
- Schliesslich sollte eine höhere maximale Richtungsabschwächung oder ein Leistungsreduktionsfaktor in der Berechnung bei der Nutzung von Beamforming berücksichtigt werden

Bundesrätin Simonetta Sommaruga
Eidgenössisches Justiz- und Polizeidepartement EJPD

per E-Mail an jonas.amstutz@bj.admin.ch

Bern, 4. April 2017

Stellungnahme zum Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

ICTswitzerland nimmt die Gelegenheit wahr, sich Vorentwurf zum Bundesgesetz über die Totalrevision des Datenschutzgesetzes (VE-DSG) zu äussern. Gerne unterbreiten wir Ihnen nachfolgend unsere Stellungnahme.

ICTswitzerland ist die Dachorganisation der Verbände sowie der Anbieter- und Anwenderunternehmen von Informations- und Kommunikationstechnologien (ICT). 27 Grossunternehmen und 21 ICT-Verbände sind an den Dachverband angeschlossen (Mitgliederliste: ictswitzerland.ch/organisation/mitglieder). ICTswitzerland vertritt die Interessen der ICT-Wirtschaft gegenüber der Öffentlichkeit und den Behörden, bezweckt die Förderung und Weiterentwicklung der Branche, fördert die führende Position der Schweiz im Bereich Forschung und Entwicklung und den Nachwuchs von qualifizierten ICT-Fachkräften. Die ICT-Branche ist mit einer Bruttowertschöpfung von CHF 28 Mrd. (2014) die sechstgrösste Wirtschaftsbranche der Schweiz.

1. Grundlegende Bemerkungen

Die Schweizer ICT-Wirtschaft unterstützt ein wirksames und modernes Datenschutzgesetz in der Schweiz – dies schafft Vertrauen zwischen Kunden und Anbietern. Akzeptanz und Vertrauen der Nutzer in den Datenschutz sind zentrale Voraussetzungen für die Fortentwicklung der digitalen Wirtschaft. Für die Wirtschaft sind Rechts- und Investitionssicherheit und eine Regulierung, die Raum für Innovation und wirtschaftliche Entwicklung lässt, von grosser Bedeutung.

Angesichts der dynamischen internationalen Entwicklung im Bereich des Datenschutzes ist es für die Schweiz zentral, dass sie den Zugang zum internationalen Markt nicht unnötig einschränkt. Damit der Schweizer Datenschutz insbesondere auch von der EU weiterhin als äquivalent angesehen werden kann, reicht es jedoch, wenn sie die grundlegenden Garantien einhält (vgl. Erw. 104 EU-DSGVO; US-EU Privacy Shields). Die Schweiz

muss sich zudem an der verbindlichen Konvention 108 des Europarats[1] und der Richtlinie (EU) 2016/680[2] orientieren.

Im Rahmen der internationalen Vorgaben ist ein Maximum an Flexibilität für den Schweizer Standort zu erhalten. Die Wirtschaft soll nicht mit unnötigem administrativem und finanziellem Aufwand belastet werden. Ein «Swiss Finish», der über die internationalen Standards oder gar über die EU Datenschutz-Grundverordnung (EU-DSGVO) hinausgeht, ist zu vermeiden. Dieser wäre aus einer gesamtheitlichen Sicht kontraproduktiv, weil solche Schweizer Besonderheiten einen einheitlichen internationalen Datenraum verhindern und damit auch zulasten der Schweizer Unternehmen wettbewerbsverzerrend wirken würden. Vor allem wirken sich überschiessende und im Geschäftsalltag nicht praktikable Regulierungen innovationshemmend aus und können der Wettbewerbsfähigkeit von Schweizer Unternehmen nachhaltig schaden.

ICTswitzerland ist überzeugt, dass die Schweiz einen wirksamen Datenschutz und die notwendige Äquivalenz mit einer schlanken Gesetzgebung erreichen kann. In Zusammenarbeit mit der branchenübergreifenden Arbeitsgruppe Datenschutz bei economiesuisse hat ICTswitzerland in mehreren Kapiteln Anpassungsbedarf identifiziert, der im Folgenden dargestellt wird.

2. Zweck (Art. 1)

Die Zweckbestimmung ist anzupassen. Gerade auch unter Berücksichtigung der Strategie «Digitale Schweiz» des Bundesrates ist der Zweck um «die Förderung des freien Verkehrs der Personendaten» zu ergänzen. Dies entspricht dem Ziel des erläuternden Berichts, dass durch die Datenschutzgesetzrevision «die Wettbewerbsfähigkeit der Schweiz gewährleistet und verbessert werden [soll], namentlich indem die Bekanntgabe von Daten ins Ausland erleichtert wird». Eine entsprechende Zielsetzung kennt auch die europäische Verordnung.

3. Geltungsbereich (Art. 2)

Berücksichtigung bereichsspezifischer Datenschutzbestimmungen
In verschiedenen Bereichen (z.B. in der Humanforschung) bestehen spezielle Bestimmungen zu datenschutzrechtlichen Fragen. Diese sind teilweise auf Verordnungsebene festgeschrieben. Es ist für die betroffenen Unternehmen zentral, dass sie sich weiterhin auf die entsprechenden Regelungen verlassen können. Es sollte festgehalten werden, dass Spezialbestimmungen im Datenschutzrecht den Regelungen des DSG vorgehen bzw. dass der Grundsatz «lex specialis» umfassend zu verstehen ist.

[1] SEV Nr.108 – Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten
[2] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates

Kein Schutz für juristische Personen
Die Abschaffung des Datenschutzes für Unternehmen analog der EU-DSGVO und Konvention 108 wird begrüsst. Dieser hat bis in der Praxis kaum eine Rolle gespielt. Einzelunternehmen und Mitglieder von Personengesellschaften, die im Handelsregister eingetragen sind, sind jedoch weiterhin vom Schutz umfasst. Es wird angeregt, dass hier dieselbe Regelung zum Geltungsbereich wie für juristische Personen gelten sollte.

Neues Missbrauchspotential beim Auskunftsrecht
Der VE-DSG sieht neu vor, dass das Datenschutzgesetz auch auf bereits rechtshängige Zivilprozesse und laufende Strafverfahren zur Anwendung gelangen soll. Dieser erweiterte Geltungsbereich birgt erhebliches Missbrauchspotential beim Auskunftsrecht (Beweisbeschaffung über die zivilprozessualen Editionsrechte hinaus). Es braucht griffige Mechanismen, welche dem Rechtsmissbrauch oder der nicht vorgesehenen Anwendung dieser Bestimmung im Zivilprozess oder im Strafverfahren entgegenstehen (vgl. Ziff. 11).

Regelung des räumlichen Anwendungsbereichs / IPR
Im VE-DSG fehlt eine Regelung zum räumlichen Anwendungsbereich des Gesetzes. Von wirtschaftlicher Seite her besteht der Wunsch, den räumlichen Anwendungsbereich nicht übermässig auszudehnen und damit den Status quo beizubehalten. Dies bedarf einer gleichzeitigen Anpassung der entsprechenden Regelung im Bundesgesetz über das Internationale Privatrecht (IPRG), damit der Geltungsbereich des Schweizerischen Datenschutzgesetzes in räumlicher Hinsicht relativiert werden kann.

4. Begriffe (Art. 3)

Definition der Personendaten
Art. 3 lit. a VE-DSG sieht keine Definition der Bestimmbarkeit vor. Es ist zu konkretisieren, was unter «bestimmbaren Personendaten» zu verstehen ist. Zudem ist wie im geltenden Recht klarzustellen, dass mit dem Begriff «Daten» stets Personendaten gemeint sind.

Einschränkung der Definition der besonders schützenswerten Personendaten
Die Ausweitung des Begriffs der «besonders schützenswerten Personendaten» auf die entsprechenden Definitionen der genetischen und biometrischen Daten geht zu weit. Der Wortlaut widerspricht den Erläuterungen im Bericht: Angedacht war die Erfassung von Daten, welche zum Zweck bearbeitet werden, eine natürliche Person eindeutig zu identifizieren. Dies entspricht auch der Stossrichtung der Konvention 108. Nach der im VE-DSG vorgeschlagenen Definition wäre beispielsweise künftig jedes Gesichtsfoto als biometrisches Datum erfasst. Die Definition ist entsprechend einzuschränken.

Einschränkung der Definition des Profiling
Die Definition des Begriffs «Profiling» ist im VE-DSG sehr breit gefasst und geht deutlich über die entsprechende Regelung der EU hinaus. In der EU-DSGVO hängt die Zulässigkeit des Profilings von der Wahrnehmung der betroffenen Interessen ab. Nur in Fällen, in denen das Profiling Teil einer automatischen Entscheidung wird und rechtliche Wirkung erzeugt, gelten andere Vorschriften. Der VE-DSG vermischt die beiden Institute: Erfasst ist auch das «menschliche», d.h. manuelle Profiling (z.B. eine schriftliche

Mitarbeiterbeurteilung oder die Alterskapitalberechnung einer Versicherung) sowie nicht-personenbezogene Daten. Dies stellt eine unzulässige Ausweitung des Geltungsbereiches dar und steht damit im Widerspruch zu Art. 2 Abs. 1 VE-DSG.

Die Definition des Begriffes ist analog der EU-DSGVO auf die automatisierte Auswertung von Personendaten zu begrenzen. Zudem ist die Auswertung bzw. Analyse keine Datenbearbeitung, die sich per se negativ auf die Persönlichkeitsrechte auswirkt. Die Bestimmung sollte daher anstatt «Auswertung» analog der EU-DSGVO den Begriff «Bewertung» verwenden.

Einführung des betrieblichen Datenschutzbeauftragten
Es besteht der Wunsch, eine Regelung zur Bezeichnung eines betrieblichen Datenschutzbeauftragten auf freiwilliger Basis vorzusehen. Dies kann mit einer entsprechenden Erleichterung bei den Pflichten unter dem DSG verknüpft werden (vgl. Ziff. 8.2). In diesem Sinne ist auch eine Definition des betrieblichen Datenschutzbeauftragten erforderlich.

5. Grundsätze (Art. 4)

Klare Terminologien
Der VE-DSG verschärft den Grundsatz der Erkennbarkeit des Zweckes unnötigerweise mit dem Zusatz der «klaren» Erkennbarkeit. Diese Anpassung an die Terminologie der EU-DSGVO ist in diesem Falle verfehlt, da die Schweizer Regelung einem unterschiedlichen Grundkonzept folgt (Erkennbarkeit im Rahmen einer klaren Zweckbindung). Die Verschärfung ist auslegungsbedürftig und produziert damit auch Rechtsunsicherheit. Der Zusatz ist nicht erforderlich und zu streichen.

Dies gilt auch für den Begriff der «eindeutigen» Einwilligung von Art. 4 Abs. 6 VE-DSG. Damit wird lediglich wiederholt, was bereits heute unter dem risikobasierten Ansatz gilt. Der Zusatz ist ebenfalls wegzulassen. Auch wann eine Einwilligung «ausdrücklich» sein soll, ist nicht klar. Jedenfalls muss auch passives Verhalten als gültige Einwilligung gelten, damit weiterhin die im Massengeschäft unumgänglichen Allgemeinen Geschäftsbedingungen (AGB) verwendet werden können. Das Erfordernis der Einwilligung für das Profiling muss gänzlich gestrichen werden (vgl. Ziff. 13).

Keine Nachführungspflicht
Die permanente Nachführungspflicht geht zu weit und ist nicht praktikabel. Der 1. Satz von Art. 4 Abs. 5 VE-DSG ist entsprechend ersatzlos zu streichen.

6. Auslandtransfer (Art. 5, Art. 6)

Unnötige Wiederholung von Grundsätzen
Art. 5 Abs. 1 VE-DSG wiederholt bereits statuierte Grundsätze und ist im Kontext von Art. 5 verwirrend und überflüssig. Der Absatz ist deshalb zu streichen.

Keine Feststellung durch den Bundesrat
Die neu vorgesehene Feststellung durch den Bundesrat, ob Daten im Ausland genügend geschützt sind, bedeutet eine unsachliche und unnötige Einschränkung. Diese Feststellung würde besser durch den Verantwortlichen, gestützt auf eigene Abklärungen und Kenntnisse, erfolgen. Die Bestimmung ist im Sinne einer geringeren Einschränkung anzupassen.

6.1. Informations- und Genehmigungspflicht (Art. 5)

Unklare und widersprüchliche Kategorisierung der Garantien
Die Unterscheidung in Art. 5 Abs. 3 VE-DSG zwischen «spezifischen» und «standardisierten» Garantien ist unklar und macht aus Sicht der Praxis keinen Sinn. Erschwerend kommt hinzu, dass die standardisierten Garantien einer Genehmigung durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) bedürfen.

Auch Binding Corporate Rules (BCR) unterliegen der Genehmigungspflicht, diese stellen aber eine Untergruppe der spezifischen Garantien dar. Für diese wiederum ist jedoch nur eine Informationspflicht vorgeschrieben. Dies ist widersprüchlich. Es sollte lediglich zwischen Standardverträgen und anderen Verträgen/Garantien unterschieden und die Pflichten entsprechend angepasst werden.

Berücksichtigung von Geheimhaltungsinteressen
Spezifische Garantien sind in der Regel in Verträgen enthalten. Es ist praxisfern und insbesondere im Zusammenhang mit dem Öffentlichkeitsgesetz (BGÖ) problematisch, wenn diese alle dem EDÖB vorgelegt werden müssen.

Keine Genehmigung durch den Beauftragten
Die Genehmigung von standardisierten Garantien oder verbindlichen unternehmensinternen Datenschutzvorschriften (BCR) durch den Beauftragten ist zu streichen. Die Genehmigungspflicht würde zu einem erheblichen Mehraufwand für die Unternehmen und gegebenenfalls zu Projektverzögerungen führen. Gleichzeitig trägt sie kaum etwas zum besseren Datenschutz bei, da das Unternehmen weiterhin selber in der Verantwortung steht. Ein grenzüberschreitender Datenfluss würde durch diese Regelung erheblich erschwert. Lediglich die EU-DSGVO (nicht die Konvention 108) sieht eine entsprechende Vorgabe vor. Hier besteht Raum für einen sich im Verhältnis zur EU-DSGVO differenzierenden Regelungsansatz.

Keine Informationspflicht bei Vorliegen standardisierter Garantien
Die pauschale Informationspflicht von Art. 5 Abs. 6 VE-DSG im Zusammenhang mit standardisierten Garantien bringt keinen Mehrwert. Es geht hier um bereits genehmigte oder anerkannte Garantien. Dies ist nicht einmal in der EU-DSGVO vorgesehen.[3] Die Bestimmung ist entsprechend zu streichen.

[3] Vgl. dazu EuGH-Entscheid Schrems und Entscheid der EU-Kommission vom 16.12.2016 (keine erneute Einwilligung im Einzelfall).

6.2. Ausnahmen (Art. 6)

Keine Einwilligung «im Einzelfall»
Die in Art. 6 Abs. 1 lit. a VE-DSG vorgesehene Ausnahme der «Einwilligung im Einzelfall» ist weder sinnvoll noch notwendig. Nach den allgemeinen Grundregeln reicht für wiederkehrende Sachverhalte bei gleichbleibender Erkennbarkeit und Erwartung eine einmalige Einwilligung. Der Zusatz «im Einzelfall» ist zu streichen. Dies gilt auch für die «Bekanntgabe im Einzelfall» (Art. 6 Abs. 1 lit. d VE-DSG).

Erweiterung der Ausnahme i. Zh. mit Verträgen
Die Ausnahmebestimmung von Art. 6 Abs. 1 lit. b VE-DSG ist mit der EU-DSGVO abzustimmen. Die Ausnahme ist auf diejenigen Fälle auszuweiten, in denen die betroffene Person nicht Vertragspartei ist, der betroffene Vertrag aber in ihrem Interesse ist oder zu ihren Gunsten abgeschlossen wurde.

Streichung Begriffe «Gericht» und «Verwaltungsbehörde»
Die Begriffe «Gericht» und «Verwaltungsbehörde» bei Art. 6 Abs. 1 lit. c VE-DSG sind zu streichen. Die Unterscheidung ist nicht erforderlich und es stellen sich schwierige Abgrenzungsfragen. Massgebend ist, dass die Datenbearbeitung zur «Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen» erfolgt.

Keine Informationspflicht bei Vorliegen eines Ausnahmetatbestandes
Die in Art. 6 Abs. 2 vorgesehene Informationspflicht, trotz Vorliegen eines Ausnahmetatbestandes, ist unverhältnismässig und zu streichen. Eine entsprechende Bestimmung ist in der Konvention 108 nicht vorgesehen. Nebst zu erwartender hoher Anzahl an Meldungen wäre auch die Information des EDÖB über heikle Verfahren und (Geschäfts-)geheimnisse problematisch (BGÖ).

7. Auftragsdatenbearbeitung (Art. 7)

Keine Vergewisserungspflicht
Die in Art. 7 neu vorgesehene Vergewisserungspflicht führt zu massivem Mehraufwand beim Outsourcing der Datenbearbeitung. Es ist unklar, welche Pflichten dem Auftragsdatenbearbeiter auferlegt werden sollen. Die Vergewisserungspflicht widerspricht dem prinzipienbasierten Ansatz des VE-DSG und die Präzisierung ist gerade in Bezug auf projektspezifische Herausforderungen kontraproduktiv. Die Bestimmung ist zu streichen. Dies gilt auch für den letzten Satz von Absatz 2 bezüglich Präzisierung weiterer Pflichten des Auftragsbearbeiters durch den Bundesrat.

Reduzierte Anforderungen an die Einwilligung
Die Anforderung einer «schriftlichen» Zustimmung ist vor dem Hintergrund der heutigen Geschäftsprozesse, insbesondere auch aufgrund der komplexen Dienstleistungsverhältnisse, nicht praxistauglich. Eine dokumentierte Zustimmung reicht aus; Schriftlichkeit i.S.v. Art. 13 OR ist nicht erforderlich. Es ist eine technologieneutrale Präzisierung vorzunehmen, dass – dies auch im Einklang mit der Bestimmung in der EU – eine generelle Einwilligung für den Beizug von Sub-Auftragsdatenbearbeitenden und eine Information im konkreten Fall ausreicht.

8. Selbstregulierung (Art. 7, Art. 8, Neu)

8.1. Empfehlungen der guten Praxis (Art. 8)

Begrüssenswerte Selbstregulierung aber keine Empfehlungen des Beauftragten
Grundsätzlich sind Empfehlungen der guten Praxis in Anlehnung an das bestehende und bewährte Konzept der Selbstregulierung der Branchen zu begrüssen. Der wesentliche Vorteil liegt darin, dass so sehr knappe oder aber sehr komplexe gesetzliche Regelungen praxisnah und operativ umsetzbar präsentiert werden können. Dazu müssen themenspezifische Wünsche der Branche tatsächlich in die Regelung einfliessen. Die im VE-DSG vorgesehene Kompetenz des EDÖB, Empfehlungen der guten Praxis auf eigene Faust auszuarbeiten, widerspricht aber dem Zweck des Instituts. Es fehlen Kontrollen und Rechtsschutzmechanismen. Entsprechend besteht die Gefahr, dass der EDÖB «falsche» oder unverhältnismässige Empfehlungen verabschiedet, ohne institutionelle Kontrolle. Aufgrund der Fiktion der Rechtmässigkeit von Art. 9 Abs. 1 VE-DSG würde er damit faktisch zum Gesetzgeber. Dem stünde verschärfend entgegen, dass eigene Empfehlungen der interessierten Kreise nur mittels Genehmigung durch den EDÖB festgelegt werden könnten. Unter der EU-DSGVO ist die Ausarbeitung von Verhaltensregeln Verbänden und anderen Vereinigungen überlassen.

Daraus ergibt sich, dass die Bestimmung der VE-DSG dahingehend anzupassen ist, dass die Initiative für Empfehlungen der guten Praxis von (Branchen-)Verbänden ausgehen muss. Dies würde der Tradition der Selbstregulierung entsprechen und brächte den Vorteil mit sich, dass solche Richtlinien von Experten mit starkem Bezug zur Praxis verfasst werden. Dies würde es ermöglichen, sachgerechte Lösungen zu entwickeln, bei denen der Beauftragte durch die Genehmigung immer noch das letzte Wort hat. Die genehmigten Empfehlungen der guten Praxis sind vom EDÖB zu publizieren.

Vermutung der Richtigkeit statt Fiktion / Geltung auch für Auftragsdatenbearbeiter (Art. 9)
Die Fiktion, welche von der Einhaltung der Empfehlungen auf die Einhaltung der Datenschutzvorschriften schliesst, ist ausserdem nicht zielführend. Es sind Konstellationen denkbar, die von den Empfehlungen nur unvollständig /unzureichend geregelt sind. Die Fiktion ist auf eine Vermutung der Richtigkeit zu reduzieren. Diese muss ebenfalls für den Auftragsdatenbearbeiter gelten.

8.2. Betrieblicher Datenschutzbeauftragter (NEU)

Einführung auf freiwilliger Basis gekoppelt mit Freistellung von Meldepflichten
Der VE-DSG verlangt richtigerweise nicht die breite Einführung eines betrieblichen Datenschutzbeauftragten. Das Institut eines betrieblichen Datenschutzbeauftragten sollte aber weiterhin vorgesehen werden. Dies als Option für die Unternehmen, kombiniert mit der Freistellung von allfälligen Meldepflichten gegenüber dem EDÖB (z.B. bei der Datenschutz-Folgenabschätzung). Ein betrieblicher Datenschutzbeauftragter könnte als zentrale Stelle die Pflichten für die Unternehmen oder ganze Unternehmensgruppen wahrnehmen. Damit liessen sich Doppelspurigkeiten vermeiden. Auch würde dadurch eine Anlaufstelle für Auskunftsbegehren geschaffen. Dies würde eine Flexibilisierung und gerade für grössere Unternehmen Erleichterungen mit sich bringen, ohne dass KMU belastet würden. Die betrieblichen Datenschutzbeauftragen sind auf freiwilliger Basis mit entsprechenden Erleichterungen für Unternehmen in das DSG einzuführen (z.B. bei Art. 15, 16 und 17 VE-

DSG). Die entsprechende Person darf jedoch im Rahmen von Sanktionen nicht übermässig exponiert werden (siehe hierzu Ziff. 14.3).

9. Daten einer verstorbenen Person (Art. 12)

Keine Regelung im DSG

Art. 12 VE-DSG erscheint im VE-DSG als Fremdkörper. Die Regelung könnte zu Rechtsunsicherheiten führen. Der Nachweis der persönlichen Beziehungen im Zusammenhang mit dem schutzwürdigen Interesse ist in der Praxis kaum zu erbringen. Für Geschäftsdaten bestehen gemäss spezialgesetzlichen Regelungen weitreichende legitime Dokumentations- und Archivierungspflichten, weshalb die pauschale Formulierung des Löschungsrechts nicht zielführend ist. Erben sind bereits durch die erbrechtliche Universalsukzession ausreichend legitimiert, geeignete, interessenwahrende Massnahmen vorzukehren. Die Bestimmung ist deshalb im VE-DSG zu streichen. Eine Regelung wäre an geeigneter Stelle (z.B. im ZGB) vorzusehen, dies aber zu einem späteren Zeitpunkt im Rahmen einer umfassenden Regelung in Bezug auf die Verfügung über Daten und nicht ausschliesslich aus einer datenschutzrechtlichen Sicht.

10. Pflichten (Art. 13 bis Art. 19)

Keine pauschale Anwendung

Die pauschale Anwendung der vorgesehenen Pflichten auf alle Geschäftsmodelle und Branchen ist nicht sachgerecht und wäre mit enormem Aufwand verbunden. Es gilt, ein gestuftes Modell vorzusehen: Strengere Bestimmungen wären dabei für Geschäftsmodelle vorzusehen, welche besonders sensible Datenbearbeitungen umfassen, wie dies typischerweise bei spezifischen Marketing-Dienstleistern und Data-Minern der Fall ist. Auch bei den Pflichten ist ein risikobasierter Ansatz vorzukehren. Zudem können branchenspezifische Regelungen weitergehende Pflichten vorsehen.

Erleichterungen für Unternehmensgruppen

Gleich strenge Regelungen für die interne Weitergabe von Daten in Konzernverhältnissen sind nicht verhältnismässig. Analog Art. 47 EU-DSGVO ist eine Bestimmung zu internen Datenschutzvorschriften für die erleichterte gruppeninterne Datenweitergabe in das DSG aufzunehmen. Dabei ist auch der Einsatz eines allfälligen internen Datenschutzbeauftragten zu berücksichtigen (vgl. Ziff. 8.2).

10.1. Informationspflichten (Art. 13)

Risikobasierte Transparenzpflicht als Leitlinie

Die erweiterten Informationspflichten auf alle Personendaten bringen Mehraufwand und führen aufgrund des öffentlich-rechtlichen Charakters der Bestimmungen und den daraus fliessenden Sanktionsfolgen zu Problemen in der Praxis. Die vorgesehene massive Ausdehnung der Informationsmenge führt zu einer Überinformation der betroffenen Personen und würde sich damit kontraproduktiv auf die Transparenz auswirken. Die Regel muss grundsätzlich im Sinne einer risikobasierten Transparenzpflicht überarbeitet werden. Es sollte zudem explizit die Möglichkeit von standardisierten Informationen (z.B. mittels AGB oder

Erklärungen auf Websites) eingeführt werden. Dies auch deshalb, weil oft nicht klar ist, worüber genau informiert werden muss.

Konkret ist die Informationspflicht auf besonders schützenswerte Daten und überdies auf Datenbearbeitungen ausserhalb des (objektiven) Erkennbarkeitshorizonts i.S.v. Art. 4 DSG der betroffenen Person zu beschränken. Ausserdem ist klarzustellen, dass sich die Information – und damit auch die Richtigkeit und Vollständigkeit der Daten – auf den Zeitpunkt der Datenbeschaffung bezieht und nicht auf nachträgliche Änderungen. Dies schliesst auch eine Pflicht zur Nachinformation klar aus. Als Kontaktdaten des Verantwortlichen muss eine klare und definierte Funktionsbeschreibung ausreichen, da die natürliche Person innerhalb einer Funktion wechseln kann.

Präzise und einheitliche Terminologien
Unklar ist die Differenzierung zwischen «Beschaffung» und «Bearbeitung» und die in Abs. 3 verwendeten Begriffe «Dritte» sowie «Empfängerinnen und Empfänger». Es sollten präzisere und einheitliche Terminologien verwendet werden. Es ist auch fraglich, warum der Vorentwurf den Begriff «Beschaffung» statt wie in der EU-DSGVO vorgesehen «Erhebung» verwendet. Dadurch können sich (nachteilige) Abweichungen im Informationszeitpunkt ergeben.

Keine Mitteilung von Identität und Kontaktdaten der Auftragsdatenbearbeiter
Die Pflicht zur Mitteilung der Identität und der Kontaktdaten sämtlicher Auftragsdatenbearbeiter ist gegenüber dem EU-Recht klar überschiessend. Sie ist weder sinnvoll noch erforderlich. Die Offenlegung der oft für untergeordnete Tätigkeiten mandatierten Auftragsdatenbearbeiter ist nur mit unverhältnismässigem Aufwand zu bewerkstelligen und greift zudem in berechtigte eigene Datenschutzinteressen sowie Geschäftsgeheimnisse der Unternehmen ein. Schliesslich ist unklar, wann genau über was informiert werden muss. Die Datenbearbeitung unter Einhaltung der gesetzlichen Vorgaben ist bereits Gegenstand von Art. 7 VE-DSG. Diese Zusatzanforderung ist zu streichen.

Keine Mitteilung bei indirekter Datenbeschaffung
Die vorgesehene Informationspflicht bei der indirekten Datenbeschaffung geht zu weit und verunmöglicht in der Praxis jede Beschaffung von Daten bei Dritten. Dem Verantwortlichen werden die relevanten Eckwerte, insbesondere die erstmalige Speicherung, oftmals gar nicht bekannt sein. Das Aufwand-Ertragsverhältnis ist damit unverhältnismässig. Darüber hinaus sind solche direkten Informationspflichten nicht erforderlich; eine allgemeine vorgängige Information des Kunden reicht aus. Die Bestimmung ist zu streichen.

10.2. Erweiterung und Präzisierung der Ausnahmen (Art. 14)

Die Ausnahmebestimmung von Art. 14 Abs. 3 lit. a VE-DSG ist zu eng gefasst. Direkte Einschränkungen ergeben sich nur selten aus einem Gesetz. Häufiger sieht ein Gesetz zwingende Abklärungspflichten vor, welche mit Geheimhaltungspflichten verbunden sind und welche damit mit einer Einschränkung der Informationspflicht einhergehen. Die Bestimmung ist zu präzisieren und mit typischen Beispielen zu ergänzen (z.B. Abklärungen im Zusammenhang mit Geldwäscherei, Terrorismusbekämpfung und Korruption). Ausserdem können sich Verpflichtungen auch aus einem Vertrag ergeben. Eine weitere Ausnahme ergibt sich bei Datenbearbeitungen, die für eine Rechtsdurchsetzung erforderlich sind. Auch dies ist zu ergänzen.

Für die Einschränkung der Berufung auf überwiegende private Interessen, d.h. auf Fälle, in denen die Personendaten nicht Dritten bekannt gegeben werden, gibt es keine sachlichen Gründe. Besonders bei Konzernverhältnissen würde daraus ein enormer administrativer Mehraufwand resultieren. Sollte die betroffene Person durch die Bekanntgabe beeinträchtigt sein, so wäre dies im Rahmen der allgemeinen Interessensabwägung von Art. 24 VE-DSG zu berücksichtigen. Die Einschränkung ist damit zu streichen.

Die Bestimmung von Art. 14 Abs. 5 VE-DSG ist nicht praktikabel und zu streichen. Diese würde dazu führen, dass ständig einzelne Interessensabwägungen überprüft werden müssten. In grossen, komplexen Organisationen ist dies nicht zu bewerkstelligen.

10.3. Automatisierte Einzelfallentscheide (Art. 15)

Begrenzung des Anwendungsbereichs und der Pflichten; insb. keine Anhörungspflicht
Die Reichweite der neu eingeführten Informations- und Anhörungspflicht sowie Auskunftsrechte bei automatisierten Einzelfallentscheiden ist zu weitgehend. Zwar kennen die Konvention 108 und die EU eine entsprechende Regelung. Der Anwendungsbereich von Art. 15 VE-DSG ist jedoch viel breiter: Der VE-DSG unterscheidet stärker zwischen Profiling und automatisierten Einfallentscheiden und sieht auch keine Ausnahmen vor. Dies hat Folgen: So wären beispielsweise Spam- und Virenscanner, Zugangskontrollen via Badge und sehr viele andere Routineentscheide erfasst, die aus Gründen der Effizienz dem Computer übertragen werden. Die Automatisierung ist ein zentraler Punkt der Digitalisierung und im heutigen wirtschaftlichen Umfeld von grundsätzlicher Bedeutung. Davon profitieren auch die Kunden, z.B. durch Objektivität der Entscheidung, schnellere Prozesse und damit besserer Nutzererfahrung sowie einer attraktiven Preisgestaltung.

Insbesondere das vorgesehene Äusserungsrecht der betroffenen Person bringt keinen Mehrwert; es ist angesichts der neu vorgesehen Informationspflicht auch schlicht unnötig und für die Unternehmen wettbewerbs- und innovationsbehindernd. In der Praxis würde es wohl regelmässig zu einer Begründungspflicht führen und damit die Vertragsfreiheit der Unternehmen über Gebühr einschränken. Die Offenlegung, wie bestimmte Entscheide zustande gekommen sind, betrifft zudem oft auch Geschäftsgeheimnisse.

Die Bestimmung ist entsprechend auf schwere Fälle, bzw. solche, die erhebliche Auswirkungen auf die betroffene Person haben, zu begrenzen. Der Wortlaut ist an die entsprechende Bestimmung in der EU-DSGVO anzupassen (insbesondere «Beeinträchtigung» statt «Wirkung» und «erhebliche» in Bezug auf beide Alternativen). Auch dann sind sinnvolle Ausnahmen notwendig, welche zumindest auf dem Verordnungsweg vorzusehen sind. Eine einmalige angemessene Information ohne ausdrückliche Einwilligung i.S.d. Gesetzessystematik ist ausreichend. Das Äusserungsrecht und der damit zusammenhängende Art. 20 Abs. 3 (Auskunftsrecht) sind zu streichen. Dies ist aufgrund des Derogationsrechts der Mitgliedstaaten der EU für die Äquivalenz nicht abträglich (vgl. Art. 22 Abs. 2 lit. c EU-DSGVO).

10.4. Datenschutz-Folgenabschätzung (Art. 16)

Beschränkung und Präzisierung / keine Pflicht des Auftragsdatenbearbeiters

Das in Art. 16 neu eingeführte Instrument der Datenschutz-Folgenabschätzung (Privacy Impact Assessment) ist zu weit gefasst. Die offene und dadurch unklare Formulierung führt dazu, dass für praktisch alle Datenbearbeitungen vorgängig aufwändige Abklärungen durchgeführt werden müssten. Besonders problematisch ist die vorgesehene Sanktionierung bei Verstoss. Analog der EU-DSGVO ist eine Konkretisierung sowie Beschränkung auf Fälle vorzunehmen, bei denen ein «hohes Risiko» besteht. Darüber hinaus ist zu präzisieren, dass ein Risiko für eine Persönlichkeitsverletzung bestehen muss. Der Begriff «oder die Grundrechte» ist sodann zu streichen: Das Schweizer Recht kennt, anders als das europäische Recht, keine direkte Drittwirkung der Grundrechte. Schliesslich ist der Auftragsdatenbearbeiter von der Pflicht auszunehmen. Dieser verfügt regelmässig nicht über die notwendigen Angaben, sondern unterliegt den Entscheidungen des Verantwortlichen.

Streichung der Meldepflicht der Datenschutz-Folgeabschätzung

Die umfangreichen Meldepflichten sind ein unnötiger «Swiss Finish»: Sie sind unverhältnismässig und greifen in die Geheimsphäre der Unternehmen ein. Die zu erwartende «Meldeflut» ist für eine angemessene Reaktion des EDÖB kontraproduktiv. Problematisch ist auch die lange Frist, innert welcher der EDÖB Einwände mitteilen oder später eine Untersuchung einleiten kann. Damit werden falsche Anreize gesetzt. In der Gesamtheit bringt die Bestimmung keinen Mehrwert, führt jedoch zu erheblichen Rechtsunsicherheiten und innovationshemmenden Verzögerungen. Die Forderung der Konvention 108, bei geplanten Datenbearbeitungen Risiken einzuschätzen, wurde bereits durch Art. 11 VE-DSG (Datensicherheit) erfüllt. Schliesslich bestehen weitere Spezialregeln, welche bestimmte Datenflüsse bereits einer anderweitigen Überwachung unterstellen (z.B. im Bankengesetz). Doppelte Überwachungen sind aus Effizienzgründen zu vermeiden.

Die umfangreichen Meldepflichten bzw. Art. 16 Abs. 3 und folglich auch Art. 16 Abs. 4 VE-DSG sind zu streichen. Eine Meldung soll erst erfolgen, wenn eine Verletzung des Datenschutzes passiert ist, nicht bereits aufgrund von Risiken. Auch die Konvention 108 verlange nicht, die Behörden von der Datenschutz-Folgenabschätzung zu informieren. Eine Ausnahme der Meldepflicht sollte zumindest für Unternehmen mit einem betrieblichen Datenschutzbeauftragten vorgesehen werden.

10.5. Meldepflichten (Art. 17)

Beschränkung auf Verstösse mit gravierenden Folgen

Die vorgesehene unverzügliche Meldepflicht im Falle sämtlicher Datenschutzverstösse (inkl. Datenverluste) an den EDÖB (Data Breach Notification) ist stark einzuschränken. Sie erfasst weit mehr Fälle als die EU-DSGVO, welche diese Pflicht nur für Verletzungen von Sicherheitsmassnahmen vorsieht, die zusätzlich zu einem Bruch oder Verlust des Gewahrsams an den Daten führen. Zudem kann die vorgesehene Ausnahme sachlogisch nie angerufen werden, da eine «falsche» Datenbearbeitung per Definition immer eine Verletzung von Persönlichkeitsrechten ist.

Eine Pflicht ohne Eingrenzung in qualitativer und quantitativer Weise würde uferlos; jeder noch so geringe Verstoss müsste gemeldet werden, um den Sanktionsfolgen zu entgehen. Der Beauftragte sähe sich mit einer weiteren Meldungsflut konfrontiert und wäre ausser Stande, allfällig wichtige Meldungen zeitgerecht zu erkennen und geeignete Massnahmen einzuleiten. Die Meldepflicht führt auch zu einem Konflikt mit dem strafrechtlichen Grundprinzip von «nemo tenetur» (vgl. Ziff. 14). Schliesslich wäre eine «unverzügliche» Meldung auch in zeitlicher Hinsicht nicht umsetzbar, da zuerst hinreichende Informationen gesammelt werden müssen. Zudem besteht die Gefahr, durch vorschnelles Handeln Geschäfts- oder Berufsgeheimnisse zu verletzen. So sieht die EU-DSGVO eine Frist von bis zu 72 Stunden vor.

Der Begriff des «Data Breach» sollte analog Konvention 108 und EU-DSGVO formuliert werden. Die Pflicht wäre damit auf Verstösse mit gravierenden Folgen zu beschränken, bei welchen ein Kontrollverlust an den Daten vorliegt. Als weiteres qualitatives Kriterium müsste die Tatsache ergänzt werden, dass durch die Meldung an den Beauftragten ein Mehrwert geschaffen werden kann. Dies z.B. mittels Unterstützung in Fällen, welche von den Verantwortlichen nicht mehr aus eigener Kraft bereinigt werden können. Weiter ist die Bestimmung durch ein quantitatives Element zu konkretisieren, z.B. auf Fälle, in welchen Daten von mindestens 100'000 Personen betroffen sind. Eine Meldung beim EDÖB muss den Schutz vor Sanktionen zur Folge haben (vgl. Ziff. 14.3).

10.6. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 18)

Anpassung der Reichweite und Überführung zu den Sicherheitsbestimmungen
Die Formulierung von Art. 18 VE-DSG geht ebenfalls über jene der EU-DSGVO hinaus. Zudem gehört diese systematisch zu Art. 11 VE-DSG (Sicherheit von Personendaten). Diese Bestimmung deckt die Anforderungen von «privacy by design» bereits. Art. 18 VE-DSG ist zu streichen, resp. in Art. 11 zu integrieren. Die Reichweite ist an das EU-Recht anzupassen.

10.7. Weitere Pflichten (Art. 19)

Verzeichnis statt allgemeine Dokumentationspflicht / Ausnahme für kleinere Unternehmen
Die allgemeine Dokumentationspflicht von Art. 19 lit. a VE-DSG ist bezüglich Inhalt und Umfang unklar und geht über die vergleichbare Bestimmung der EU hinaus. Die Pflicht ist analog der EU-DSGVO auf die Pflicht zur Erstellung «eines Verzeichnisses für regelmässige Datenbearbeitungen» einzuschränken. Die Pflicht, Datenschutzverstösse zu dokumentieren, ist zu weitgehend. Darüber hinaus ist auch eine Ausnahme der Pflicht für kleinere Unternehmen (z.B. analog EU mit weniger als 250 Mitarbeitenden oder am Umsatz gemessen) vorzusehen, sofern sie in Bezug auf den Datenschutz keine risikoreiche Tätigkeit ausüben. Aus systematischen Gründen sollte auch diese Bestimmung in Art. 11 VE-DSG integriert werden.

Beschränkung der Informationspflicht an Dritte
Die Reichweite der neu vorgesehenen Pflicht, Dritten die Berichtigung, Löschung oder Vernichtung von Daten zu melden, geht sehr weit und ist in der Praxis nicht umsetzbar. Eine solche Meldepflicht ist von Konvention 108 nicht und von der EU-DSGVO nicht in dieser Form vorgesehen. Die EU-DSGVO kennt eine entsprechende Meldepflicht nur unter gewissen Voraussetzungen im Zusammenhang mit dem «Recht auf Vergessen». Der VE-DSG erfasst demgegenüber auch unbedeutende Vorgänge; im täglichen Arbeitsprozess werden ständig Daten berichtigt, gelöscht oder vernichtet (z.B. weil ein Kunde bezahlt hat oder die Daten schlicht keine Relevanz

mehr haben). Die Auswirkungen dieser Meldepflicht wurden offenbar unterschätzt. Zu deren Bewältigung müsste eine neue Infrastruktur aufgebaut werden, welche sämtliche Empfänger über Jahrzehnte hinweg verwaltet. Eine betroffene Person ist besser in der Lage zu beurteilen, welche Daten für welche Empfänger (noch) von Interesse sind. Gerade solche Informationsansprüche der betroffenen Person sind aber bereits unter Art. 25 VE-DSG vorgesehen. Die Informationspflicht an Dritte ist analog der EU-DSGVO auf Fälle zu beschränken, in welchen die betroffene Person die Nachinformation aus berechtigten Gründen verlangt hat.

11. Auskunftsrecht (Art. 20)

Massnahmen gegen missbräuchliche Auskunftsbegehren
Die Ausweitung des Auskunftsrechts auf sämtliche Datenbearbeitungen und hängige Verfahren bringt grosse Aufwendungen mit sich. Umso mehr, weil ein Auskunftsbegehren im Datenschutzsystem der Schweiz nie unverhältnismässig sein kann, da auch untergeordnete Datenschutzinteressen für einen Anspruch ausreichen. Gerade auch die vorgesehene umfassende Kostenlosigkeit des Auskunftsrechts führt zu Fehlanreizen: Es sind keine Massnahmen vorgesehen, welche es den Unternehmen erlauben würden, dem Missbrauch des Auskunftsrechts zu datenschutzfremden Zwecken Einhalt zu gebieten (vgl. Ziff. 3).

Es sind griffige Massnahmen gegen den Missbrauch des Auskunftsrechts zu datenschutzfremden Zwecken vorzusehen: Die Kostenlosigkeit ist zu relativieren, so z.B. bei unverhältnismässigem Aufwand und bei Ersuchen zu nicht ausschliesslich datenschutzrechtlichen Zwecken. Zudem sind weitere Mechanismen zur Verhinderung des Auskunftsrechts bei offensichtlich nicht datenschutzrechtlichen Zwecken vorzusehen (z.B. bei Art. 21 VE-DSG).

Einschränkung der Informationspflicht bei automatisierten Einzelfallentscheiden
Eine «Rechenschaftspflicht» in Bezug auf automatisierte Entscheide in der vorgesehenen detaillierten Form ist unverhältnismässig: Informationen darüber, wie bestimmte Entscheide zustande kommen, gehören zum Geschäftsgeheimnis. Durch die gewählte Formulierung wäre jedes Ergebnis, d.h. jeder Entscheid, erfasst. Dies würde zu einem zusätzlichen Administrativaufwand führen, ohne dass damit mehr Transparenz geschaffen würde. Im Gegenteil: Kunden würden Informationen erhalten, mit denen sie gar nichts anzufangen wissen (z.B. warum sie eine Werbeanzeige nicht erhalten haben).

Die geforderte Information über Vorliegen einer automatisierten Einzelfallentscheidung (Art. 20 Abs. 2 lit. e VE-DSG) sollte in allgemeiner Weise erfolgen. Die Bestimmung von Art. 20 Abs. 3 VE-DSG sollte in Art. 15 VE-DSG integriert werden. Dessen Grundsätze («erhebliche Auswirkung») wären dabei einzuhalten. Es muss klargestellt werden, dass das Auskunftsrecht nur von der jeweils tatsächlich betroffenen Person ausgeübt werden kann. Zudem ist ein Verweis auf die Einschränkungen des Auskunftsrechts bzw. der Informationspflichten (Art. 21 i.V.m. 14 VE-DSG) anzubringen.

12. Ausnahmetatbestände (Art. 21)

Ausweitung der Ausnahmen
Die vorgesehenen Ausnahmetatbestände gemäss Art. 14 VE-DSG sind zu eng formuliert und nicht konsistent. Die Informationspflicht sollte immer entfallen, wenn die Information nicht möglich oder unzumutbar ist. Eine Beschränkung auf Fälle der indirekten Beschaffung oder in denen keine Weitergabe an Dritte erfolgte, ist nicht nachvollziehbar. Die Bestimmung ist entsprechend anzupassen.

Es sind Ausnahmen, auch in Hinblick auf die rechtsmissbräuchliche Geltendmachung des Auskunftsrechts, für folgende bearbeiteten Daten vorzusehen:

- Daten, welche die betroffene Person bereits erhalten hat, z.B. in Form von Verträgen, Abrechnungen und Korrespondenzen;
- Aufgrund einer gesetzlichen Pflicht bearbeitete Daten, z.B. zur Verhinderung von Geldwäscherei, Terrorismusfinanzierung und Korruption;
- Daten, welche vom Auskunftspflichtigen als Geschäftsgeheimnisse qualifiziert werden;
- Rein intern bearbeitete Daten;
- Daten über Drittpersonen;
- Unter rechtsmissbräuchlichen Umständen herausverlangte Daten, insbesondere die Geltendmachung des Auskunftsrechts ohne erkennbaren sachlichen Grund oder mit häufiger, sachlich nicht nachvollziehbarer Wiederholung.

Übergabe der Informationen an Dritte bei Missbrauchsverdacht (Neu)
Um Missbräuche zu verhindern, ist zudem vorzusehen, dass bei begründetem Verdacht auf Missbrauch die herauszugebenden Personendaten einem Dritten (bspw. dem EDÖB) übergeben werden können. Dieser würde anstelle des Gesuchstellers die Einhaltung bzw. Verletzung des Datenschutzes prüfen. Eine Möglichkeit bestünde darin, dass der EDÖB den Entscheid über Herausgabe in Form einer anfechtbaren Verfügung vorlegt (vgl. analoge Regelung in Art. 8 Abs. 2 BPI).

13. Besondere Bestimmungen für die Datenbearbeitung durch private Personen (Art. 23, Art. 24)

Keine ausdrückliche Einwilligung beim Profiling (Art. 23)
Gemäss Art. 23 Abs. 2 lit. d VE-DSG gälte Profiling automatisch als Persönlichkeitsverletzung, wenn nicht vorgängig eine ausdrückliche Einwilligung eingeholt wird. Diese gesetzliche Vermutung stellt einen unbegründeten partiellen Paradigmenwechsel im Schweizer Datenschutzrecht dar (von grundsätzlicher Erlaubnis der Datenbearbeitung unter Einhaltung bestimmter Voraussetzungen zum Verbot mit Erlaubnisvorbehalt). Das Erfordernis der ausdrücklichen Einwilligung beim Profiling ist entsprechend zu streichen. Durch eine entsprechende Information kann genug Transparenz geschaffen werden. Eine Regelung hat unter Art. 15 VE-DSG zu erfolgen.

Klare und erweiterte Rechtfertigungsgründe (Art. 24)
Der Ausdruck «möglicherweise» in Art. 24 Abs. 2 VE-DSG schafft Rechtsunsicherheit. Die aktuelle Bestimmung (Art. 13 Abs. 2 DSG) wurde unnötigerweise geändert und sollte beibehalten werden.

Art. 24 Abs. 2 lit. a VE-DSG sollte analog Art. 6 Abs. 1 lit. b VE-DSG Verträge berücksichtigen, die zu Gunsten oder im Interesse der betroffenen Person geschlossen werden.

14. Aufsicht und Sanktionen (Art. 50 bis 55)

Das vorgeschlagene Sanktionsmodell stösst branchenübergreifend auf Kritik und ist aus Sicht der ICT-Wirtschaft nicht geeignet. Entsprechend wird zu diesem Kapitel umfassend Stellung genommen und es wird eine Grobskizze für einen alternativen Vorschlag für ein im Datenschutzgesetz zu integrierendes Sanktionsmodell.

14.1. Ausgangslage

Anders als der VE-DSG setzen die Konvention 108 und die EU-DSGVO in erster Linie auf Verwaltungssanktionen gegen Unternehmen. Bei der Regelung der Sanktionierung von Datenschutzverletzungen besteht gemäss den europäischen Bestimmungen ein erheblicher Spielraum: Die Konvention verlangt im Wesentlichen geeignete gerichtliche und nicht-gerichtliche Sanktionen und Rechtsmittel (Art. 10 E-SEV 108). Die EU-DSGVO und auch die Richtlinie 2016/680 sprechen von wirksamen, verhältnismässigen und abschreckenden Sanktionen. Es ist dabei den Mitgliedsstaaten überlassen, zu entscheiden, ob Sanktionen strafrechtlicher oder verwaltungsrechtlicher Art sind (Erw. 149 und 152).

14.2. Kritik am Vorentwurf und weitere Überlegungen

Die im VE-DSG vorgesehenen Sanktionen und insbesondere der Weg über das Strafrecht sind nicht zielführend.

Persönliche Strafbarkeit der Mitarbeitenden
Die Mitarbeitenden eines Unternehmens geraten durch die persönliche Strafbarkeit zu stark in den Fokus der Sanktionen. Verschärft wird dies durch die Höhe der Bussen und die vorgesehene Möglichkeit, sogar fahrlässiges Handeln zu bestrafen. Damit wird der risikobasierte Ansatz, der mit der Revision verfolgt wird, untergraben.

Strafrechtliche Sanktionen führen dazu, dass Mitarbeitende in Zukunft selbständig jeden (möglichen) Verstoss bei den Behörden melden müssen. Dies birgt das Risiko, dass sie sich gegenseitig anzeigen, um nicht selbst ins Visier der Strafbehörde zu geraten. Der VE-DSG bietet zudem Dritten viele Anknüpfungspunkte (sobald eine Datenerhebung stattgefunden hat), um Anzeige zu erstatten. Dies kann zum Unterlaufen der intern definierten Datenschutz-Governance und zu Unruhen innerhalb der Unternehmen führen sowie entsprechende Reputationsschäden nach sich ziehen.

Verurteilte Mitarbeitende wären sowohl intern als auch extern stark exponiert. Es dürfte daher mittelfristig schwierig werden, qualifiziertes Personal zu finden, das bereit ist, die Verantwortung mit den einhergehenden Risiken zu tragen. Die Folge wäre ein sukzessives Abfallen der Qualität im Bereich der Datenbearbeitung.

Die persönliche Strafbarkeit der Mitarbeitenden entspricht auch nicht der von anderen Schweizer Gesetzen vorgesehen Linie (vgl. KG, UWG, FMG, BEHG), bei welchen der Fokus klar auf der Sanktionierung der Unternehmen liegt.

Die strafrechtliche Sanktionierung würde schliesslich insbesondere die KMU stark belasten. Bei übersichtlichen Verhältnissen ist die Identifikation fehlbarer Mitarbeitender relativ einfach; entsprechend bestünde ein Anreiz für die Strafverfolgungsbehörden, gerade bei solchen Unternehmen unverhältnismässig streng vorzugehen.

Verstoss gegen strafrechtliche Grundprinzipien
Problematisch sind die im VE-DSG vorgesehenen Mitwirkungspflichten angesichts des im Strafrecht vorherrschenden Grundsatzes des «nemo tenetur» bzw. des Selbstbelastungsverbotes. Die Pflicht, Datenschutzverstösse zu melden, käme faktisch einer Pflicht zur Selbstanzeige gleich. Der VE-DSG geht von einer verschuldensunabhängigen Sanktionierung aus und steht damit im Widerspruch zum Verschuldensprinzip: Bei Vorliegen des objektiven Tatbestandes wird direkt darauf geschlossen, dass auch der subjektive Tatbestand erfüllt ist. Viele der Pflichten des VE-DSG und damit auch die daraus abgeleiteten Straftatbestände sind offen formuliert (vgl. Art. 16 Abs. 1 VE-DSG: «…vorgesehene Datenbearbeitung [führt] voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person»). Dies ist mit dem strafrechtlichen Bestimmtheitsgebot bzw. einer hinreichenden Voraussehbarkeit einer Strafbarkeit nicht vereinbar.

Umfang von potentiellen Verstössen und Meldungen
Datenbearbeitungen stellen innerhalb der Unternehmen eine alltägliche Aktivität dar. Unternehmen können im Zeitalter der Digitalisierung nicht mehr wählen, ob eine entsprechende Handlung vorzunehmen ist oder nicht. Damit unterscheidet sich das Datenschutzrecht beispielsweise vom Kartellrecht. Im VE-DSG sind kaum Erheblichkeitsschwellen vorgesehen. Folglich würde jede geringfügige Unregelmässigkeit in alltäglichen Datenbearbeitungsvorgängen eine Datenschutzverletzung darstellen. Die daraus resultierende Mitteilungsmenge an den Beauftragten sowie die drastischen Sanktionsfolgen wären höchst problematisch.

Strafkatalog
Im Kern entspricht der Strafkatalog grundsätzlich den europäischen Bestimmungen. Hingegen werden die Berufspflichten erheblich verschärft und es wird sogar eine Freiheitsstrafe als Sanktion vorgesehen. Diese Ausweitung des Berufsgeheimnisses ist als überschiessende Bestimmung klar abzulehnen; es können in dieser Hinsicht nicht alle Berufe mit jenen von Art. 321 StGB gleichgesetzt werden.

Fazit
Die strafrechtlichen Sanktionen des VE-DSG, die gegen Mitarbeiter eines Unternehmens ausgesprochen werden können, sind weder verhältnismässig noch zielführend. Diese stehen im Widerspruch zu einer Vielzahl von schweizerischen strafprozessualen Prinzipen. Die auf Risikoausgleich ausgerichteten Möglichkeiten des VE-DSG werden damit ausgehöhlt und der Interessensausgleich wird unnötig eingeschränkt. Gesamthaft geht das vorgeschlagene strafrechtliche Sanktionsmodell damit deutlich über die im europäischen Raum vorgesehenen Sanktionen, die in erster Linie verwaltungsrechtlicher Natur sind, hinaus.

14.3. Vorschlag der Wirtschaft für ein Sanktionsmodell im DSG

Aufgrund der vorangehenden Überlegungen sprechen wir uns für ein alternatives Sanktionsmodell aus. Nicht strafrechtliche Sanktionen gegen Individuen, sondern Verwaltungsstrafen gegen Unternehmen sollen dabei im Vordergrund stehen.

Auch bei Verwaltungsstrafen ergeben sich verschiedene Problemfelder, gerade auch aus rechtsstaatlicher Sicht. Das nachfolgend skizzierte Modell berücksichtigt diese und schlägt ein auf die spezielle Konstellation des Datenschutzes angepasstes, verwaltungsrechtliches Sanktionsmodell vor. Dieses soll effizient ausgestaltet sein, die richtigen Anreize setzen und den Anforderungen an ein faires Verfahren entsprechen.

Grundsatz: verwaltungsrechtliche Sanktionen gegen Unternehmen
Das DSG soll bei Verstössen gegen die Datenschutzbestimmungen eine Sanktionierung der Unternehmen vorsehen. Anknüpfungspunkt sind dabei Organisationsmängel im Unternehmen. Lediglich subsidiär soll eine strafrechtliche Verfolgung von Mitarbeitenden möglich sein. Anzeigen sollen in der Regel durch die Unternehmen selbst erstattet werden. Im Ergebnis würde eine Anpassung des Sanktionsziels die Situation für die Datenbearbeitenden im Sinne einer Verbesserung des Datenschutzes im Unternehmen massgeblich entschärfen.

Weiter soll eine Sanktionierung der Mitarbeitenden nur bei direkt vorsätzlichem Handeln, das sich gegen die Interessen des Unternehmens und/oder der betroffenen Person richtet, in Frage kommen. In diesem Zusammenhang ist eine Abstimmung mit den bereits im BT StGB vorgesehenen Strafbestimmungen erforderlich. Diese dürften für die Bestrafung der natürlichen Person meist schon ausreichen (z.B. Verletzung des Geschäftsgeheimnisses und unbefugte Datenbeschaffung). Der Kreis der potentiell strafrechtlich verantwortlichen Mitarbeitenden müsste zum Vornherein eingeschränkt werden (entsprechend Art. 29 StGB).

Angepasste Rolle des EDÖB und verbesserte Gewaltentrennung durch eine neu zu bildende Spruch-Behörde
Eine Behörde, die gleichzeitig über Untersuchungs- und Spruchkompetenzen verfügt (wie bei Sanktionen mit verwaltungsrechtlichem Charakter üblich), hat die Tendenz, eine mit dem Prinzip der Gewaltenteilung nur schwer vereinbare Machtfülle zu erlangen. Die Verwaltungssanktionen sollten daher nicht von der Untersuchungsbehörde verhängt werden.

Die Ausstattung des EDÖB mit Spruchkompetenzen, sogar die im VE-DSG bereits vorgesehene Ausstattung mit Verfügungskompetenzen, kann dazu führen, dass der EDÖB zu mächtig wird. Zusätzlich besteht die Gefahr, dass eine vertrauensvolle Zusammenarbeit mit den Unternehmen im Bereich der wichtigen Beratung beeinträchtigt wird. Ein auf Vertrauen basierender Austausch mit den Unternehmen ist für die Tätigkeit des Beauftragten jedoch von grundsätzlicher Bedeutung, dies umso mehr, als ihm gemäss VE-DSG die Aufgabe zukommt, Empfehlungen der guten Praxis zu erlassen.

Die Verfügungskompetenzen sowie die Sanktionskompetenz könnten entsprechend in einer neu zu bildenden «Datenschutz-Kommission» gebündelt werden. Diese könnte beispielsweise dem EDI oder EJPD angehängt sein. Ausschliesslich dieser kämen nebst der Sanktionskompetenz auch die Verfügungskompetenzen zu, dies

gerade auch im Bereich vorsorglicher Massnahmen. Das Verhältnis zwischen «Datenschutz-Kommission» und EDÖB müsste präzisiert werden, insbesondere in Bezug auf die Überwachungs- und Untersuchungskompetenzen des Beauftragten i.S.v. Art. 40 f. VE-DSG.

In dieser Struktur würde der EDÖB seine bisherigen Aufgaben wahrnehmen und eine Vorselektion der ihm zugetragenen Fälle machen. Sollte sich in einem Fall eine mögliche Strafbarkeit abzeichnen, würde er die Angelegenheit der «Datenschutz-Kommission» weiterleiten. Bei Verfahren auf dieser zweiten Stufe würde die verwaltungsrechtliche Mitwirkungspflicht des Beauftragten wegfallen. Gegen Entscheide dieser Spruchbehörde stünde den Betroffenen der Weg zum Bundesverwaltungsgericht als Rechtsmittelinstanz offen.

Strafkatalog

Der Strafkatalog ist mit jenem der EU-DSGVO abzugleichen, soll jedoch nicht darüber hinausgehen. Folgende Anpassungen sind erforderlich:

- Konkretisierung / Streichung der zu offen formulierten Tatbestände;
- Beschränkungen und Anpassungen bei den Pflichten des Verantwortlichen und Auftragsbearbeiter sind beim Strafkatalog zu berücksichtigen;
- Fokus auf wesentliche Bedrohung für die Privatsphäre der betroffenen Person;
- Einführung einer Erheblichkeitsschwelle, welche sich z.B. an der Schwere der Persönlichkeitsverletzung (in quantitativer oder qualitativer Hinsicht) oder an der Höhe des entstandenen Schadens in Bezug auf die betroffene Person orientiert. Zu einem schweren Verstoss gegen das Datenschutzgesetz gehört auch, dass die unbefugte Datenbearbeitung vorsätzlich vorgenommen wurde;
- Verzicht auf die Pönalisierung von reinen Fahrlässigkeitsdelikten;
- Streichung der Strafandrohung bei verweigerter Mitwirkung / Kooperation ab 2. Stufe des Verfahrens (siehe unten);
- Beschränkung der beruflichen Schweigepflicht auf Fälle, in denen die betroffene Person eine berechtigte Erwartung der Geheimhaltung hat (z.B. aufgrund eines Vertrages).

Mitwirkungspflichten und Strafmilderungsgründe

Neben der im Vorentwurf vorgesehenen Pflicht, Datenschutzverstösse bei den Behörden zu melden, besteht für die Unternehmen im verwaltungsrechtlichen Verfahren generell eine Mitwirkungspflicht. Wie oben kritisiert, läuft die Idee der anschliessenden Bestrafung im Rahmen eines Strafverfahrens diesem Konzept entgegen und verstösst zusätzlich gegen das Selbstbelastungsverbot. Ein kooperatives Verhalten, das letztlich einer raschen Schadensminderung dienen soll, muss gefördert werden. Unternehmen, die den Beauftragten über eine Verletzung der Datenschutzbestimmungen informieren, mit den Behörden kooperieren, Fehler aktiv korrigieren und grössere Risiken zu verhindern suchen, sollen mit einer Reduktion der Sanktion oder gar dem Absehen von einer Sanktion rechnen können (vgl. auch Art. 49a Abs. 2 KG). Dieser auf Schadensminderung ausgerichtete Ansatz entspricht den modernen Grundsätzen der Corporate Governance und fördert gleichzeitig das Ziel, ein hohes Datenschutzniveau zu erreichen.

Gründe, die strafmildernd wirken sollten, wären:

- Compliance-Defense: Implementierung eines tauglichen Compliance-Programmes;

- Einhaltung der Corporate Governance: Einhalten sämtlicher unternehmensinternen Richtlinien, Ausschöpfen der betriebsinternen Eskalationsleiter und Interventionsmöglichkeiten, Meldung eines möglichen Verstosses sowie kooperatives Verhalten gegenüber den Behörden;
- Handeln nach Treu & Glauben durch vernünftigen Umgang mit komplexen Regeln: Angemessene Umsetzung komplexer Verhältnisse (z.B. viele Beteiligte und grenzüberschreitende Verhältnisse) unter Berücksichtigung des «state of the art»;
- Wahrung berechtigter Interessen: Güterabwägung im Fall von Pflichtenkollision mit anderen zwingenden Rechtsregeln (z.B. unter Zeitdruck angewendete etablierte Notfallszenarien (BCM) im öffentlichen Interesse zur Abwendung eines Unternehmenskonkurses; vgl. Notstand, Art. 17 StGB);
- Rechts- und Sachverhaltsirrtum (vgl. Art. 13 und 21 StGB);
- Strafrechtliche Verfolgung eines Mitarbeitenden. Eine Anzeige gegen einen direktvorsätzlich handelnden Mitarbeitenden durch das Unternehmen muss im Rahmen der Bestrafung des Unternehmens, insbesondere im Hinblick auf das Schuldprinzip, berücksichtigt werden;
- Aktive Schadensverminderung und Zusammenarbeit mit den Behörden.

Sanktionen

Datenbearbeitungen gehören zur täglichen Arbeit der Unternehmen. Datenschutzverletzungen können dementsprechend im Rahmen des Tagesgeschäftes geschehen. Dies muss bei der Festlegung der Sanktionshöhe einen Einfluss haben. Hierbei sind die gesamten Umstände des Einzelfalles zu berücksichtigen, so z.B. die Schwere und die Auswirkungen des Verstosses sowie die oben genannten Strafmilderungsgründe. Ebenso muss, in Anlehnung an die EU-DSGVO, eine Konkurrenzklausel eingefügt werden: Bei gleichen oder miteinander verbundenen Datenbearbeitungsvorgängen, durch die vorsätzlich mehrere Bestimmungen des VE-DSG verletzt wurden, darf der Gesamtbetrag der Busse nicht denjenigen Betrag übersteigen, der für die schwerwiegendste Verletzung vorgesehen ist.

15. Übergangsfristen (Schlussbestimmungen, Abs. 10)

Im VE-DSG fehlt eine umfassende Übergangsregelung. Die neuen und revidierten Bestimmungen werden die Prozesse der Unternehmen bedeutend beeinflussen. Es ist deshalb eine allgemeingültige Übergangsbestimmung von zwei Jahren aufzunehmen. Von einer Rückwirkung ist abzusehen.

16. Zusammenfassung der Kernanliegen

Die Schweizer Datenpolitik und damit auch die Datenschutzregulierung sollte sich an den übergeordneten Zielen der Strategie «Digitale Schweiz» des Bundesrates orientieren: Zu berücksichtigen ist insbesondere der Nutzen der Daten für den digitalen Fortschritt und die Ausschöpfung des wirtschaftlichen Potentials im Interesse der Konsumenten und Unternehmen. Eine einseitige Orientierung an potentiellen Risiken wäre verfehlt. Im Grundsatz sind Behinderungen von Innovation und Entwicklungen durch Datenschutzvorgaben zu vermeiden.

Im Datenschutzgesetz ist für die Schweizer Unternehmen ein Maximum an Flexibilität und ein Minimum an Belastung zu wahren. Spielräume im Verhältnis zum internationalen Recht und das etablierte System der Selbstregulierung sind so weit als möglich zu nutzen. Die im Vergleich zum EU-Raum überschiessenden Regelungen sind anzupassen. Dabei soll die Totalrevision auch genutzt werden, um bestehende Bestimmungen zu hinterfragen und an die technologische Entwicklung anzupassen.

Zusammenfassend lassen sich in Bezug auf die VE-DSG folgende vier Hauptforderungen festhalten:

- Diverse **Informations- und Meldepflichten** gehen zu weit. Sie bedeuten unverhältnismässigen Aufwand und generieren eine regelrechte «Flut» an Informationen und Meldungen. Abzulehnen sind auch die damit verbundene Offenlegung von Geschäftsgeheimnissen und die Pflicht, sich selbst zu belasten. Gesamthaft wirken sich die vorgeschlagenen Pflichten innovations- und wettbewerbshindernd aus. Sie sind dem vom Vorentwurf angestrebten risikobasierten Ansatz entsprechend substantiell zu reduzieren. Dies betrifft insbesondere automatisierte Einzelfallentscheide, Datenschutz-Folgenabschätzungen und Meldungen von Datenschutzverstössen. Darüber hinaus braucht es eine Relativierung der Kostenlosigkeit des Auskunftsrechts und weitere, griffige Massnahmen, um dem Missbrauch des Datenschutzrechtes zu datenschutzfremden Zwecken entgegenzuwirken.
- Ein weiterer umfassender Kritikpunkt ist das vorgeschlagene **Sanktionssystem**: Private, strafrechtliche Sanktionen sind weder verhältnismässig noch zielführend. Es ist ein tragbares, mit den rechtsstaatlichen Grundsätzen vereinbares Sanktionssystem zu implementieren. Gleichzeitig ist eine zu grosse Machtfülle des EDÖB zu verhindern.
- Der Begriff «**Profiling**» ist auf automatisierte Bewertungen von Personendaten einzuschränken und die Bedingungen dazu sind stark zu reduzieren (Information statt Einwilligung).
- Die Initiative für Empfehlungen der guten Praxis muss zwingend von (Branchen-)Verbänden ausgehen. Die **Selbstregulierung** ermöglicht es mittels Bezug zur Praxis, sachgerechte Lösungen zu entwickeln. Der betriebliche Datenschutzbeauftragte ist auf freiwilliger Basis mit entsprechenden Erleichterungen für Unternehmen in das DSG einzuführen.

Wir danken Ihnen für die Aufmerksamkeit, die Sie unseren Anliegen entgegenbringen.

Freundliche Grüsse

Andreas Kaelin
Geschäftsführer ICTswitzerland