simsa, Heinrichstrasse 235, 8005 Zürich

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

per E-Mail: Jonas.amstutz@bj.admin.ch

Zürich, 31. März 2017

Stellungnahme der simsa – Swiss Internet Industry Association zum Vorentwurf für das totalrevidierte Datenschutzgesetz

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Die simsa – Swiss Internet Industry Association ("simsa") ist der Interessenverband der Schweizer Internet-Dienstleistungsunternehmen. Wir danken Ihnen für die Möglichkeit zur Stellungnahme zum Vorentwurf des Datenschutzgesetzes ("VE-DSG"). In unserer Stellungnahme gehen wir exemplarisch und ohne Anspruch auf Vollständigkeit auf diejenigen Vorschläge des Vorentwurfs ein, welche für die Internetindustrie in der Schweiz besonders relevant sind.

Das Wichtigste in Kürze:

Starker Datenschutz und Datensicherheit sind wichtige Grundpfeiler für den Erfolg digitaler Geschäftsmodelle in der Schweiz. Der Austausch von Personendaten mit unseren Nachbarländern und anderen wichtigen Handelspartnern muss möglich bleiben, weshalb ein inhaltlich gegenüber der EU gleichwertiger Datenschutz zu erhalten ist. Das Schweizer Datenschutzgesetz (DSG) aus dem Jahr 1992 basiert auf allgemeinen Grundsätzen der Datenbearbeitung, die sich in der Praxis bewährt haben und die sich bisher auch erfolgreich auf digitale Sachverhalte anwenden liessen. Gemäss Beschluss der EU-Kommission vom 26. Juli 2000 verfügt die Schweiz über ein angemessenes Datenschutzniveau. Dieser Beschluss bleibt auch unter der ab 25. Mai 2018 verbindlichen EU Datenschutz-Grundverordnung (Verordnung EU 2016/679; DSGVO) weiterhin gültig. **Eine Teilrevision des DSG genügt, um den Herausforderungen der Digitalisierung zu begegnen und einen gegenüber der EU angemessenen Datenschutz zu erhalten.**

Für die Schweiz **im internationalen Verhältnis direkt verbindlich ist das (revidierte) Übereinkommen des Europarates (SEV 108)** zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener

Daten. Das Übereinkommen bedingt, wenn überhaupt, lediglich wenige Änderungen im DSG. Solange die Schweiz die SEV 108 einhält besteht auch für die EU kein Grund, auf den Angemessenheitsentscheid zurückzukommen und diesen zu revidieren. **Für eine Übernahme der in der DSGVO detailliert geregelten administrativen Pflichten bei der Datenbearbeitung sowie für hohe Bussen besteht in der Schweiz kein Anlass.**

Geradezu unverständlich ist, dass der VE-DSG verschiedene Pflichten der DSGVO nicht nur übernimmt, sondern diese gar noch verschärft. In dieser Stellungnahme weisen wir nur auf die wichtigsten dieser strengeren Regelungen hin, welche die Geschäftstätigkeit von Online-Dienstleistern und Betreibern digitaler Geschäftsmodelle in der Schweiz bedrohen. **Sämtliche Verschärfungen gegenüber den Regelungen der DSGVO sind aus dem VE-DSG zu entfernen.** Vor allem auf überschiessende Neben- und Administrativpflichten ist zu verzichten. Solche Pflichten erhöhen den Aufwand für die Schweizer Anbieter von Kommunikations- und Werbe-Diensten, IT-Beratung, Hosting-, Cloud-Lösungen und anderen Dienstleistern für digitale Geschäftsprozesse. Die Administrativpflichten stärken auch den Persönlichkeitsschutz der betroffenen Personen kaum. Um die Attraktivität des Dienstleistungsstandorts Schweiz zu erhalten, sind Pflichten und Einschränkungen für Schweizer Anbieter zu vermeiden, welche sogar über das von der EU geforderte Mass hinausgehen.

Besonders standortschädlich und abzulehnen ist das vorgeschlagene Sanktionswesen mit neuen Straftatbeständen. Der Verzicht auf drakonische Sanktionen im Stile der DSGVO (Bussen bis zum höheren Betrag von EUR 20 Mio. oder 4% des letzten weltweit erzielten Jahresumsatzes) ist zwar zu begrüssen. Der VE-DSG setzt darauf, die Verletzung von administrativen Nebenpflichten neu als Straftatbestände auszugestalten. Ins Visier geraten damit die natürlichen Personen in der Schweiz, welche für die Datenbearbeitung in Unternehmen verantwortlich sind. Nur wenn sich diese nicht identifizieren lassen, soll subsidiär das Unternehmen mit maximal CHF 100'000.— gebüsst werden. Für global tätige Online-Plattformen ohne Niederlassung in der Schweiz wäre eine solche Busse im Vergleich zu einer Sanktion in der EU ein kleines Übel. Schweizer Unternehmen – besonders KMU – hingegen müssten ihre Mitarbeiter mit grossem Compliance-Aufwand schützen und würden sich im Zweifel für eine konservativere Methode der Datenbearbeitung entscheiden. **Im Ergebnis wäre der VE-DSG gut für Beratungsunternehmen und Anwaltskanzleien, nicht aber für innovative Unternehmen, die in der Schweiz datengestützte Geschäftsmodelle betreiben möchten.**

Im Einzelnen:

Die Auftragsdatenbearbeitung ist nicht unnötig zu erschweren (Art. 7 ff. VE-DSG):

Die Informationspflichten sind auf ein verhältnismässiges Mass zu beschränken. Die vorgesehenen Pflichten sind zu unbestimmt. Die aktive Information muss z.B. alle Angaben umfassen, die für die betroffene Person "erforderlich" sind (Art. 13 Abs. 2 VE-DSG). Längere Datenschutzerklärungen bedeuten nicht automatisch eine bessere Information der betroffenen Person. Daher verfehlt die Informationspflicht das Regelungsziel der Stärkung von Kontrollmöglichkeiten der Betroffenen. Die sehr weit formulierte Informationspflicht widerspricht dem risikobasierten Ansatz, wie sie der Vorentwurf im Rahmen der Transparenzanforderung gemäss Art. 4 VE-DSG vorsieht.

Die Pflicht zur Information über die Identität und Kontaktangaben der Auftragsbearbeiter ist überschiessend (Art. 13 Abs. 4 VE-DSG). Der Verantwortliche müsste die betroffene Person, z.B. bei jedem Wechsel des Kommunikations-, Werbe-, IT-, Hosting- oder Beratungs-Dienstleisters, über die Identität und Adresse des neuen Anbieters informieren. Diese Information erhöht den Datenschutz und die Datensicherheit für die betroffene Person nicht, sondern führt zu einer kontraproduktiven Informationsflut. Die Information ist zudem in einer arbeitsteiligen, digitalen Geschäftswelt nicht praktikabel. Weder die SEV 108 noch die DSGVO verlangen die Angabe der Identität der Auftragsbearbeiter. Es ist nicht einzusehen, weshalb sich die Schweiz freiwillig einen massiven Standortnachteil auferlegen sollte.

Die Pflicht zur permanenten Datenüberprüfung ist in der Praxis nicht erfüllbar (Art. 4 Abs. 5 und Art. 19 Bst. b VE-DSG). Vor allem Auftragsbearbeiter sind von der Datenquelle zu weit entfernt, als dass sie Änderungsbedarf an den von ihnen bearbeiteten Daten erkennen können. Die Tätigkeit des Auftragsbearbeiters erfolgt immer im Auftrag des Verantwortlichen. Daher kann höchstens der Verantwortliche für die Richtigkeit der zur Verfügung gestellten Daten sorgen.

Auf strafrechtlich sanktionierte Informationspflichten des Auftragsbearbeiters gegenüber Datenempfängern ist zu verzichten (Art. 19 Bst. a VE-DSG). Daten werden tagtäglich angepasst, ergänzt oder gelöscht, weil die Daten nicht mehr notwendig sind oder an Relevanz verloren haben. Beispiele dafür sind die Archivbereinigung, der Abschluss der Leistungserbringung, die Begleichung der offenen Forderung durch den Kunden oder die Auflösung einer Geschäftsbeziehung. Es ist unverhältnismässig, wenn der Verantwortliche und der Auftragsbearbeiter in allen Fällen einer Berichtigung, Löschung oder Vernichtung von Daten alle Datenempfänger nachinformieren müssen. Die Informationspflicht ist auf Fälle zu begrenzen, in welchen die betroffene Person ein Begehren um Datenanpassung aufgrund schutzwürdiger Interessen gestellt hat. Die Mitteilung an Dritte soll höchstens dann erfolgen, wenn die betroffene Person dies aus berechtigten Gründen verlangt. Der Verantwortliche entscheidet über Zweck, Mittel und Umfang der Bearbeitung und ist damit auch in der Position, über den Bedarf für eine Datenanpassung zu befinden. Aus diesem Grund soll der Verantwortliche und nicht der Auftragsbearbeiter für die Mitteilung zuständig sein. So sieht es auch die EU vor (Art. 19 DSGVO).

Datenschutz-Folgenabschätzung, Privacy by Design und Privacy by Default sind keine Aufgaben des Auftragsbearbeiters (Art. 16 und 18 VE-DSG). Der Verantwortliche entscheidet über eine bestimmte Geschäftsaktivität und die damit zusammenhängende Datenbearbeitung. Die Pflichten zur Datenschutz-Folgenabschätzung, zur Sicherstellung des Datenschutzes durch Technik (Privacy by Design) und durch datenschutzfreundliche Voreinstellungen (Privacy by Default) setzen zu einem frühen Zeitpunkt in der

Planung an. Der Auftragsbearbeiter ist in diese Entscheidungsprozesse meist nicht involviert. Hat der Auftragsbearbeiter einen entsprechenden Auftrag vom Verantwortlichen erhalten, verfügt er meist trotzdem nicht über alle relevanten Informationen. Die genannten Pflichten sind für den Auftragsbearbeiter daher kaum umsetzbar. Gleichzeitig stellen die Sanktionsdrohungen für den Auftragsbearbeiter unverhältnismässig hohe Risiken dar. Auch die EU beschränkt die genannten Pflichten auf den Verantwortlichen (Art. 25 und 35 DSGVO). Die Schweiz sollte die in der Schweiz ansässigen Dienstleister nicht gegenüber den EU-Anbietern benachteiligen. Sofern der Verantwortliche Schutzmassnahmen festlegt, wird er diese zudem auch vertraglich auf den Auftragsbearbeiter überbinden, soweit sie die Auftragsbearbeitung betreffen.

Die Einwilligungsvoraussetzung für eine Unterbeauftragung ist nicht praktikabel (Art. 7 Abs. 3 VE-DSG). In einer arbeitsteiligen Welt muss der Auftragsbearbeiter flexibel und zeitnah Unteraufträge vergeben können (z.B. eine Marketingagentur für die verschiedenen Elemente und Teilleistungen einer online Kampagne, ein Registrar und Hosting-Anbieter für verschiedene Elemente seines Domain- und Hosting-Geschäfts oder ein IT-Beratungsunternehmen für die verschiedenen Teilleistungen eines Mandates wie Softwareentwicklung, Datenauswertungen etc.). Er gewährleistet dabei gegenüber seinem Auftraggeber die Einhaltung der Pflichten durch die Unterauftragnehmer. Eine Pflicht zur vorgängigen Einholung der Einwilligung durch den Verantwortlichen ist praxisfern und nicht notwendig.

Der Auslandtransfer ist nicht unnötig zu verzögern und zu erschweren (Art. 5-6 VE-DSG):

Die zahlreichen Melde- und Genehmigungspflichten für die Bekanntgabe ins Ausland sind unverhältnismässig und fördern den Datenschutz nicht. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) würde zahlreiche für ihn kaum relevante Meldungen erhalten. Solche Mitteilungen bewirken für die betroffenen Personen keinen stärkeren Schutz. Die verpflichteten Verantwortlichen und Auftragsbearbeiter müssten in ihren Meldungen an den EDÖB unnötigerweise Geschäftsgeheimnisse offenbaren (z.B. betreffend hängiger ausländischer Verfahren). Für die Verpflichteten bestehen dabei unverhältnismässige Risiken, da die übermittelten Informationen dem Öffentlichkeitsgesetz unterliegen können. Ein Auftragsbearbeiter wird zudem nur auf Auftrag und Instruktion des Verantwortlichen tätig. Es ist der Verantwortliche, welcher die beauftragten Bearbeitungen als Teil seiner Geschäftsaktivität plant und über die erforderlichen Informationen verfügt. Es macht für eine zeitnahe Benachrichtigung und Aktivierung des EDÖB keinen Sinn den Auftragsbearbeiter für Praktiken in die Pflicht zu nehmen, die der Verantwortliche alleine bestimmt. Für einen Schweizer Kommunikations- oder Werbe-Dienstleister, Web-Designer oder Cloud-Anbieter, der von seiner Kundin ausserhalb Europas Daten erhält und speichert bzw. bearbeitet, ist unter der vorgeschlagenen Regelung zudem nicht klar, ob er für den Re-Export der Daten in das Land der Kundin eine neue vertragliche Grundlage (im Sinne von Abs. 3) benötigt. Die Bussendrohung stellt für den Auftragsbearbeiter eine unzumutbare Unsicherheit dar. Die strafrechtlich sanktionierten Melde- und Genehmigungspflichten sind insbesondere für Auftragsbearbeiter zu löschen.

Die vorgesehene Frist von sechs Monaten (anstelle der bis anhin 30 Tage) zur Prüfung von standardisierten Garantien und unternehmensinternen verbindlichen Vorschriften ist kontraproduktiv. Viele Anbieter können nicht so lange auf einen Bescheid warten und werden sich auf eine andere Basis für den Auslandtransfer stützen oder die geplante Aktivität aufgeben. Diese Frist ist für den EDÖB nicht einmal verbindlich, was zu einer unzumutbaren Rechtsunsicherheit und einem Nachteil für Schweizer Anbieter führt. Es ist zudem nicht einzusehen, warum bei spezifischen Garantien der EDÖB nur informiert werden muss, bei standardisierten Garantien aber eine langwierige Vorprüfung vorgeschrieben ist. Gerade standardisierte Garantien sowie unternehmensinterne verbindliche Vorschriften haben das Potential zur Entwicklung von wichtigen Best

Practices. Davon profitieren wiederum die betroffenen Personen. Vorbildliche Anbieter, die für ihre Branche solche Standards durch regen Gebrauch etablieren möchten, sollen nicht durch unverhältnismässig lange Prüffristen des EDÖB blockiert werden.

Das DSG soll die Datenbekanntgabe auch im Zusammenhang mit einem Vertrag im Interesse der betroffenen Person erlauben. Die Bekanntgabe ins Ausland ist ausnahmsweise erlaubt, wenn die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Daten des Vertragspartners handelt. Unter der DSGVO ist die Bekanntgabe auch für den Abschluss oder die Erfüllung eines bloss im Interesse der betroffenen Person geschlossenen Vertrages möglich (Art. 49 Abs. 1 Bst. c DSGVO). Die Schweiz soll diese erweiterte Ausnahme den eigenen Anbietern nicht vorenthalten.

Missbrauchspotential beim Auskunftsanspruch ist zu vermeiden (Art. 20 VE-DSG):

Der Auskunftsanspruch ist auf ein verhältnismässiges Mass an Daten zu beschränken. Die vorgesehene Auskunftspflicht umfasst alle Angaben zur Aufbewahrungsdauer, die Identität und Kontaktdaten aller Auftragsbearbeiter, das Ergebnis, Zustandekommen und die Auswirkungen von Entscheidungen, die auf irgendeiner Art von Datenbearbeitung beruhen. Dieser sehr weit gefasste Anspruch eröffnet Missbrauchspotential: Querulatorische Gesuche oder Anfragen zu datenschutzfremden Zwecken werden zunehmen. Das vorgeschlagene Auskunftsrecht geht weit über das verhältnismässige Mass und die Regelung der DSGVO hinaus. Die DSGVO beschränkt z.B. den zusätzlichen Anspruch auf Auskunft bei automatisierten Einzelfallentscheiden auf Fälle, in denen besonders schützenswerte Personendaten bearbeitet werden oder der Entscheid eine rechtliche Wirkung oder andere erhebliche Beeinträchtigung für die betroffene Person hat. Der ufer- und voraussetzungslose Auskunftsanspruch im VE-DSG steht in einem Missverhältnis zur Belastung der Auskunftspflichtigen. Aufgrund der vorgesehenen Bussendrohung, können Bearbeiter auch missbräuchliche Anfragen faktisch nicht mehr zurückweisen.

Für Auskunftsansprüche ist ein Kostenersatz vorzusehen. Ohne den Ausschluss des DSG in hängigen Zivilprozessen und laufenden Strafverfahren (Art. 2 Abs. 2 VE-DSG) eröffnet der Vorentwurf weiteres Missbrauchspotential: Mittels Auskunftsbegehren kann eine Verfahrenspartei kostenlos umfangreiches Beweismaterial für datenschutzfremde Zwecke beschaffen. Damit lassen sich z.B. die im Zivilprozess bestehenden Anforderungen für Editionsbegehren umgehen. Querulatorische oder wiederholte Anfragen können grosse Ressourcen binden. Ohne Kostenersatz geht das Risiko einseitig zu Lasten der Auskunftspflichtigen. Staatliche Behörden können bei einer Auskunft nach dem Öffentlichkeitsgesetz einen Kostenbeitrag verlangen. Selbst die DSGVO sieht zumindest bei wiederholten Anfragen den Kostenersatz vor (Art. 15 Abs. 3 DSGVO).

Auf unverhältnismässige Anforderungen an das Profiling ist zu verzichten (Art. 3 Bst. F und Art. 23 Abs. 2 Bst. d VE-DSG):

Informations- und Anhörungspflichten sollen auf automatisierte Entscheide mit erheblichen Auswirkungen beschränkt werden. In einem ersten Schritt ist der Begriff des Profiling einzuschränken auf die automatisierte Auswertung von personenbezogenen Daten, deren Ergebnis wiederum Personendaten sind. Dies sieht auch die DSGVO vor (Art. 4 Abs. 4 DSGVO). Profiling an sich hat für die betroffene Person kaum direkte Auswirkungen. Rechtliche Anforderungen sollen daher, wenn überhaupt, nur an die Verwendung der Ergebnisse anknüpfen, z.B. für automatisierte Entscheide. Erfasst wären aber potentiell sehr viele Routineverfahren, die im Rahmen der fortschreitenden Digitalisierung aus Effizienzgründen automatisiert werden, z.B. Prozesse zur Vertragsabwicklung. Die zusätzlichen administrativen Hürden für die Verpflichteten

sollen in einem angemessenen Verhältnis zum Schutzbedürfnis der betroffenen Personen stehen. Die Pflichten bei automatisierten Einzelfallentscheiden sind daher in einem zweiten Schritt auf Entscheide zu beschränken, welche unmittelbare und erhebliche Auswirkungen auf die Persönlichkeitsrechte der betroffenen Person haben. Das DSG soll zudem weitere Ausnahmen von den Pflichten bei automatisierten Einzelfallentscheiden aufnehmen, wie dies auch die EU vorsieht (Art. 22 DSGVO). Darunter fallen z.B. Entscheidungen, die für den Abschluss oder die Erfüllung von Verträgen mit der betroffenen Person erforderlich sind.

Der Geheimnisschutz ist auf Berufe mit spezialgesetzlicher Schweigepflicht und eine berechtigte Geheimniserwartung einzuschränken (Art. 52 VE-DSG):

Eine Geheimhaltungspflicht soll nur greifen bei beruflichen Schweigepflichten, die unabhängig von Art. 52 VE-DSG bestehen. In den spezialgesetzlich erfassten Berufszweigen (z.B. Arzt, Anwalt) ist für alle Beteiligten klar, dass eine besondere Vertraulichkeit notwendig ist, z.B. für Patientendaten. Für viele andere Geschäftsfelder, die standardmässig Personendaten erfassen und bearbeiten (z.B. Online-Händler, Werbe-Dienstleister etc.), ist dies nicht der Fall. Früher oder später können praktisch alle Berufszweige mit geheimen Personendaten in Berührung kommen. Die vorgeschlagene Regel schliesst Anbieter damit weitgehend von jeglicher Nutzung der beschafften Daten aus. Die Bussendrohung für derart weit gefasste Pflichten ist unverhältnismässig. Sie ist zu beschränken auf berufliche Schweigepflichten, die ein anderes Gesetz vorschreibt. Wie bei anderen beruflichen Geheimnispflichten, muss eine Befreiung durch die Aufsichtsbehörde möglich sein.

Die Ausweitung des Geheimnisschutzes auf alle Personen, welche geheime Daten kommerziell bearbeiten ist überschiessend. Nicht einmal die EU sieht eine derart strenge Regelung vor. Dienstleister in den Bereichen der datengestützten Beratung und der personalisierten Online-Werbung (z.B. Betreiber von Werbenetzwerken, Dienstleister im Bereich digitales Marketing), aber auch Hosting- und Cloud-Anbieter könnten solche Dienstleistungen kaum mehr in der Schweiz anbieten. Die Sanktionsdrohung wäre ein weiterer massiver Standortnachteil für die Schweiz.

Nur diejenigen geheimen Daten sind zu schützen, für die der Geheimnisherr auch eine berechtigte Erwartung an die Geheimhaltung hat. Sofern zwischen dem Geheimnisherrn (d.h. der betroffenen Person) und dem Bearbeiter als Geheimnisträger z.B. eine vertragliche Grundlage für die Bearbeitung besteht, soll auch die Bearbeitung und entsprechende Offenlegung möglich sein.

Selbstregulierung ist zu fördern und nicht zu verordnen (Art. 8-9 VE-DSG):

Nur Empfehlungen der guten Praxis aus der jeweiligen Branche selbst sind zielführend. Das DSG soll die Selbstregulierung in Eigeninitiative der jeweiligen Branchen fördern. Die Kompetenz dazu muss bei den interessierten Kreisen liegen, nicht beim EDÖB. Die Befugnisse des EDÖB zur Ausarbeitung und Genehmigung von Empfehlungen sind zu weitgehend und können zu praxisfernen Alleingängen führen. Nicht praktikable Empfehlungen schwächen den Datenschutz eher, als dass sie die Persönlichkeitsrechte der betroffenen Personen wirksam schützen. Erfahrungen mit Schweizer Selbstregulierungen haben gezeigt, dass echte Brancheninitiativen am wirksamsten sind. Auch der erläuternde Bericht nennte als Erfolgsbeispiele (S. 53) die Verhaltenskodizes der Brancheninitiative des Schweizerischen Verbandes der Telekommunikation für verbesserten Jugendmedienschutz in den neuen Medien und zur Förderung der Medienkompetenz in der Gesellschaft sowie den Code of Conduct Hosting unserer Organisation.

Die freiwillige Benennung eines betrieblichen Datenschutzbeauftragten zeigt die Erfüllung der Sorgfaltspflichten des Unternehmens. Es ist richtig, dass die Schweiz auf die zwingende Benennung eines

betrieblichen Datenschutzbeauftragten verzichtet. Das DSG soll aber Unternehmen, die freiwillig eine solche Sorgfaltsmassnahme ergreifen, von gewissen Pflichten entbinden. Die mit der Einsetzung eines betrieblichen Datenschutzbeauftragten gezeigte Sorgfalt ist zudem bei allfälligen Sanktionsbemessungen zu berücksichtigen.

Meldepflicht bei Datenschutzverletzungen muss verhältnismässig sein (Art. 17 VE-DSG):

Die Meldepflicht ist auf Datenschutzverletzungen mit erhöhtem Risiko für eine Vielzahl von Personen zu beschränken. Anders als in der EU, stellt der Wortlaut des Schweizer Vorentwurfs alle unbefugten Datenschutzbearbeitungen unter die Meldepflicht. Aus Gründen der Verhältnismässigkeit soll die Meldepflicht nur in Fällen eines Datenverlusts, einer unbefugten Offenlegung oder eines unbefugten Datenzugangs mit erhöhtem Risiko für die Persönlichkeitsrechte einer grösseren Zahl von betroffenen Personen greifen. Andernfalls rechtfertigen sich das Einschalten und Aktivwerden des EDÖB nicht. Die Verpflichteten sollen die dazu nötige Einschätzung der Risiken und Anzahl Betroffener nach sorgfältigen Massstäben aber in eigenem Ermessen durchführen können. Eine Meldung soll ohne unnötige Verzögerung erfolgen, wobei sachliche Gründe (z.B. Massnahmen zur Schliessung des Lecks, zur technischen Untersuchung etc.) eine Verzögerung rechtfertigen können.

Zu weitgehend ist auch die Meldepflicht an Dritte. Der Vorentwurf enthält die Schweizer Besonderheit, wonach jeder Verantwortliche und Auftragsbearbeiter allfällige Drittempfänger der Daten über Verletzungen des Datenschutzes informieren muss. Diese Mitteilung hat unabhängig davon zu erfolgen, ob eine Meldung an den EDÖB oder an die betroffene Person notwendig ist. Die EU sieht keine solche Pflicht vor (Art. 19 DSGVO). Diese Mitteilung beinhaltet ein enormes Potential zur Rufschädigung. Es ist nicht einzusehen, weshalb die Schweiz derartige Verschärfungen einführen soll, die keine Erhöhung des Datenschutzes aber massive administrative Aufwendungen für Verantwortliche und Auftragsbearbeiter bewirken.

Auf unverhältnismässige Sanktionen einseitig zulasten der Schweizer Anbieter ist zu verzichten (Art. 50-53 VE-DSG):

Der Verzicht auf hohe Bussen führt nicht zum Verlust des Angemessenheitsbeschlusses der EU. Das SEV 108 verlangt lediglich die "wirksame" Umsetzung (Art. 4 Abs. 1 und 3 Bst. a SEV 108) und "geeignete" Sanktionen (Art. 10 SEV 108). Das DSG muss keine hohen Bussen für Administrativpflichten vorsehen, um diesen Anforderungen gerecht zu werden. Die Verfügungskompetenz des EDÖB und die Sanktion bei Widerhandlungen gegen rechtskräftige Verfügungen (Art. 292 StGB) reichen als wirksame Durchsetzungsmassnahmen aus.

Die selbständige Sanktionierung von Administrativpflichten stärkt den Datenschutz nicht und ist unverhältnismässig. Die zahlreichen selbständig sanktionierten, administrativen Pflichten (Art. 50 und 51 VE-DSG) erhöhen den administrativen Aufwand und das finanzielle Risiko für Schweizer Anbieter. Diese Pflichten bleiben aber weitgehend ohne direkte Wirkung für den Schutz der Persönlichkeitsrechte der betroffenen Personen.

Hohe Schweizer Bussen bedrohen einseitig Schweizer Anbieter. Die vorgeschlagene Sanktionsregelung bedeutet für in der Schweiz ansässige KMU eine stärkere finanzielle Belastung, als für grosse, internationale Konzerne: Für internationale Anbieter ohne Schweizer Niederlassung ist der Anreiz grösser, die natürliche Person nicht identifizierbar zu halten. Für Schweizer Anbieter liesse sich demgegenüber regelmässig leichter feststellen, wer als natürliche Person zur Verantwortung gezogen werden kann. Damit sind die Risiken gerade für Geschäftsführer und leitende Angestellte von Schweizer Unternehmen grösser als für

internationale Konkurrenten. Eine grosse Rechtsunsicherheit für die verpflichteten Unternehmen besteht zudem aufgrund fehlender Harmonisierung und sehr unterschiedlicher datenschutzrechtlicher Erfahrung der zuständigen kantonalen Strafbehörden.

Die Ausweitung des Strafkatalogs widerspricht der Schweizer Rechtstradition. Unter dem geltenden DSG sollen Datenschutzverstösse nur ausnahmsweise mit strafrechtlichen Sanktionen geahndet werden (Botschaft des Bundesrates vom 23. März 1988 zum DSG, BBl 1988 II 413, 484). In der Schweizer Rechtstradition ist nicht zwingend eine Androhung von Strafen notwendig, damit gesetzliche Verpflichtungen als verbindlich aufgefasst werden. Den Verpflichteten drohen bei Nichtbefolgen der Administrativpflichten an sich bereits regelmässig Rechtsnachteile, z.B. wegen fehlender Nachweise in einem Verfahren. Zudem sind die administrativen Pflichten im Vorentwurf sehr unbestimmt (z.B. die Dokumentationspflicht), was eine Bestrafung rechtsstaatlich problematisch macht. Die Ausweitung des Sanktionskatalogs für Administrativpflichten schadet auch dem offenen und zielgerichteten Dialog zwischen Datenbearbeitern und dem EDÖB.

Für die Berücksichtigung der Anliegen der Internetindustrie zur Schaffung einer verhältnismässigen und praxistauglichen Datenschutzregulierung danken wir Ihnen im Voraus und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

simsa – Swiss Internet Industry Association

Andrej Vckovski — Präsident

Rolf Auf der Maur — Vizepräsident