Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ
Direktionsbereich Öffentliches Recht
Fachbereich Rechtsetzungsprojekte und -methodik

Anhörung zum Entwurf zu einer Änderung der Verordnung zum Bundesgesetz über den Datenschutz und zu einer Verordnung über die Datenschutzzertifizierungen: Zusammenstellung der Ergebnisse

1. Allgemeine Bemerkungen zur Anhörung

Die Eidg. Räte haben am 24. März 2006 eine Revision des Bundesgesetzes über den Datenschutz (DSG, SR 235.1) verabschiedet (Referendumsvorlage BBl 2006 3547). Die Referendumsfrist ist unbenutzt verstrichen. Im Hinblick auf die Inkraftsetzung der Revision ist das Verordnungsrecht anzupassen. Die Änderungen sind zwar überwiegend technischer Natur, aber dennoch bedeutsam für die Praxis, insbesondere in zahlreichen Bereichen der Wirtschaft. Aus diesem Grund hat das Eidg. Justiz- und Polizeidepartement beschlossen, eine Anhörung nach Artikel 10 Vernehmlassungsgesetz (SR 172.061) durchzuführen. Die Anhörung wurde am 27. Februar 2007 eröffnet und dauerte bis Ende Mai 2007.

46 Organisationen (vgl. Liste im Anhang) waren eingeladen, zu den Entwürfen Stellung zu nehmen.

Beim EJPD sind 32 Stellungnahmen eingegangen (vgl. Liste im Anhang). Davon stammen 22 von offiziell konsultierten Kreisen, 10 Antworten erfolgten von nicht offiziell begrüssten Organisationen oder Privaten. 7 eingeladene Organisationen teilten den Verzicht auf eine Stellungnahme mit oder hatten keine Bemerkungen zu den beiden Vorlagen.

2. Gegenstand der Anhörung

Die Revision des Datenschutzgesetzes bedingt auf Verordnungsebene einige Änderungen. Diese betreffen in erster Linie die Pflicht zur Anmeldung der Datensammlungen sowie die Pflicht zur Information des Datenschutz- und Öffentlichkeitsbeauftragten über verwendete Garantien oder konzerninterne Datenschutzregeln, wenn Personendaten in Staaten bekannt gegeben werden, die nicht über eine Datenschutzgesetzgebung verfügen, welche einen genügenden Schutz gewährleistet. Darüber hinaus ist die Datenschutzverordnung aufgrund von Artikel 11a Absatz 6 DSG mit Bestimmungen über die Funktion des oder der betrieblichen Datenschutzbeauftragten zu ergänzen.

Die im Artikel 11 des revidierten DSG vorgesehenen Datenschutzzertifizierungen erfordern ebenfalls gewisse Umsetzungsbestimmungen. Da es sich dabei um eine vollständig neue Materie handelt, soll dazu eine eigene Verordnung erlassen werden. Diese Verordnung regelt namentlich die Akkreditierung von Zertifizierungsstellen sowie die Minimalanforderungen, denen die Datenschutzzertifizierung von Organisation und Verfahren bzw. von Produkten (Hardware, Software, Systeme für automatisierte Datenbearbeitungsverfahren) genügen müssen. Weder der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte noch eine andere staatliche Stelle werden selbst Zertifizierungen durchführen.

3. Zusammenfassung der Stellungnahmen zu den wesentlichen Punkten

3.1 Entwurf zu einer Änderung der Verordnung zum Bundesgesetz über den Datenschutz

3.1.1 Allgemeine Bemerkungen

Eine Bundesbehörde (EKK) und 9 Organisationen stimmen dem Revisionsentwurf ausdrücklich zu (ACSI, CP, Datenschutzforum, FER, kf, RVK, SDV, SGB, santésuisse).

Eine Organisation lehnt die Vorlage ausdrücklich ab (privatim). Sie ist der Auffassung, dass es der Entwurf versäumt, in wichtigen Bereichen die gesetzlichen Vorgaben konkret und konsequent umzusetzen.

Die weiteren Stellung nehmenden Kreise äussern sich nicht zu der Vorlage insgesamt.

3.1.2 Pflicht zur Anmeldung von Datensammlungen (Art. 3 und 4)

Art. 3 des Entwurfs regelt die Modalitäten der Anmeldung; Art. 4 legt – im Rahmen der von Art. 11a Abs. 5 Bst. b revDSG vorgesehenen Delegation an den Bundesrat – die Ausnahmen von der Meldepflicht fest.

Zu der geringfügigen Anpassung von *Art. 3* erfolgte lediglich eine Detailbemerkung.

Eine Organisation begrüsst die in *Art. 4* vorgesehenen Ausnahmen ausdrücklich (FER). Fünf Organisationen et un privé verlangen eine Erweiterung des Ausnahmekataloges bzw. deren Angleichung an den für die Bundesorgane geltenden Katalog (Datenschutzforum, santésuisse, swico, SVV, swissbanking und Belser). Swissbanking und swico beantragen insbesondere, dass Datensammlungen von der Anmeldepflicht auszunehmen sind, die Daten von Personen enthalten, die über die Bearbeitung nach Art. 7a DSG informiert worden sind oder die ihr ausdrücklich zugestimmt haben. Mehrere Organisationen verlangen Detailanpassungen.

Fünf Organisationen sprechen sich gegen die in Art. 4 Abs. 2 vorgesehene Pflicht aus, eine Liste aller nicht der Meldepflicht unterliegenden Datensammlungen zu führen (Groupe Mutuel, santésuisse, swissbanking, SVV, swico). Es wird vor allem argumentiert, dafür fehle dem Bundesrat die rechtliche Grundlage.

3.1.3 Information des Beauftragten bei Datenbekanntgaben bei bestimmten Übermittlungen in ausländische Staaten (Art. 5)

Artikel 5 des Entwurfs konkretisiert die Bestimmung von Art. 6 Abs. 3 revDSG, nach der der Beauftragte zu informieren ist, wenn Daten gestützt auf besondere – insb. vertragliche – Garantien oder konzerninterne Datenschutzregeln in einen ausländischen Staat bekannt gegeben werden, der nicht über eine Gesetzgebung verfügt, die einen angemessenen Schutz gewährleistet. Er sieht insbesondere vor, dass eine einmalige Information genügt, wenn Modellverträge verwendet werden, die der Beauftragte erstellt oder anerkannt hat.

Keine der Stellungnahmen hat sich gegen diese Bestimmung in ihrer Gesamtheit ausgesprochen. Es erfolgten ausschliesslich Detailbemerkungen. So verlangen beispielsweise zwei Organisationen, dass eine konkrete Frist festgelegt werden solle,

innert der der Beauftragte die vertraglichen Garantien oder die konzerninternen Datenschutzregeln überprüfen muss bzw. nach deren Ablauf diese von Gesetzes wegen als akzeptiert gelten, wenn er nicht interveniert (Datenschutzforum, swico). Die Regelung, dass die Informationspflicht als erfüllt gilt, wenn vom Beauftragten erstellte oder anerkannte Modellverträge verwendet werden und der Beauftragte in allgemeiner Form über diese Tatsache informiert wird, wurde in zwei Stellungnahmen ausdrücklich begrüsst (FER, Bär&Karrer). Eine Organisation war der Meinung, der Beauftragte solle nicht nur bei der Erarbeitung von Modellverträgen und Standardvertragsklausels tätig werden bzw. mitwirken, sondern auch bei der Erarbeitung von Modellen für konzerninterne Datenschutzregeln (swico).

3.1.4 Betrieblicher Datenschutzberater (Art. 12a und 12b)

Die Artikel 12a und 12b stellen Regeln für das von Art. 11a Abs. 5 Bst. e revDSG neu vorgesehene Instrument des betrieblichen Datenschutzberaters auf.

Die vorgesehene Regelung wurde dem Grundsatz nach nicht bestritten. Es erfolgte indessen eine Anzahl von Detailbemerkungen. So sprachen sich namentlich vier Organisationen sowie ein Privater betreffend die deutsche Fassung dagegen aus, von "Datenschutzberater" zu sprechen und sprechen sich für ein Festhalten am in Art. 11a DSG verwendeten Begriff "Datenschutzverantwortlicher" aus (privatim, RVK, Datenschutzforum, SVV, Belser). Eine Organisation hat sich dagegen für die Verwendung des Begriffs des "Datenschutzberaters" ausgesprochen (swico).

Drei Organisationen (swissbanking, swico, SVV) sowie ein Privater (Bär&Karrer) haben sich auch gegen das in Art. 12b Abs. 1 Bst. b vorgesehene Recht jeder Person ausgesprochen, auf ein entsprechendes Gesuch hin Einsicht in die vom Datenschutzberater zu führende Liste der Datensammlungen nach Art. 11a Abs. 3 DSG nehmen zu können. Sie verlangten Streichung (SVV) oder Beschränkung des Zugangsrechts auf betroffene Personen (Bär&Karrer) bzw. den Beauftragten (swissbanking, swico, Eventualantrag SVV).

3.2 Entwurf zu einer Verordnung über die Datenschutzzertifizierungen

Eine Bundesbehörde (EKK) und 3 Organisationen (acsi, kf, SDV) stimmen dem Entwurf ausdrücklich zu. 5 Organisationen äussern sich skeptisch (CP, FER, CVAM, IVSK, swico), wobei eine davon der Datenschutzzertifizierung von Produkten ausdrücklich zustimmt (swico). Eine Behörde (SAS) und 3 Organisationen (Datenschutzforum, privatim, SGS) sprechen sich gegen den Entwurf aus. Die übrigen Stellungnahmen äussern sich nicht zum Entwurf in seiner Gesamtheit.

Ausdrücklich begrüsst wird in mehreren Stellungnahmen der Verzicht auf ein offizielles Datenschutz-Qualitätszeichen (EKK, acsi, CP, CVAM, FER, kf, Belser).

Die skeptischen Stellungnahmen argumentieren vor allem, die Vorlage sei schwer verständlich und sehr technisch formuliert (CP, CVAM). Die FER ist der Ansicht, die vorgesehenen Voraussetzungen für eine Zertifizierung bedeuteten einen administrativen Aufwand, der, im Vergleich zum damit verbundenen Vorteil, kaum verhältnismässig sei (ähnlich auch swico). Auch die IVSK fragt sich, worin der Mehrwert der Zertifizierung liegen könnte.

Die Ablehnung wird wie folgt begründet: Für die SAS ist nicht akzeptabel, dass die Vorlage kein offizielles Datenschutz-Qualitätszeichen (DSQ) vorsieht (auch der

EDÖB und RVK verlangen, die Verordnung solle ein offizielles DSQ vorsehen, ohne indessen den Entwurf abzulehnen). Eine Organisation vertritt die Auffassung, das Zertifizierungsverfahren sei in der vorgeschlagenen Form untauglich (privatim). Nur eine unabhängige Stelle könne eine unabhängige Zertifizierung gewährleisten, daher müsse der EDÖB selbst die Zertifizierungen vergeben oder zumindest eine verbindliche Kontrolle der Prüfberichte vornehmen. Das Datenschutzforum und die SGS sind der Ansicht, dass der Entwurf die Mindestanforderungen an die Zertifizierung nicht klar regelt. Die von einer Arbeitsgruppe unter Leitung des EDÖB entworfene konkretisierende Regelung hätte die notwendige Klarheit geschaffen.

4. Beurteilung des Entwurfs zu einer Änderung der Verordnung zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11)

4.1 Modalitäten des Auskunftsrechts (Art. 1 Abs. 2)

Drei Organisationen (FER, IVSK, santésuisse) begrüssen die neu vorgesehene Möglichkeit, das Auskunftsgesuch und die Mitteilung der fraglichen Informationen auch auf elektronischem Wege abwickeln zu können. Santésuisse verlangt dazu, dass Abs. 2 dahingehend präzisiert wird, dass die betroffene Personen nur dann einen Anspruch darauf hat, das Auskunftsgesuch auf elektronischem Weg stellen zu können, wenn der Inhaber der Datensammlung dies ausdrücklich vorsieht.

Zwei Organisationen (swissbanking, swico) sprechen sich gegen die vorgeschlagene Änderung aus. Sie sind der Auffassung dass sie Risiken für die betroffenen Personen und Probleme bei der Umsetzung für die Inhaber der Datensammlung mit sich bringt. Sie schlagen daher vor, auf diese Neuerung zu verzichten, oder eventuell Abs. 2 wie folgt zu ergänzen:

> "*[2] Das Auskunftsbegehren sowie die Auskunftserteilung können auf elektronischen Weg erfolgen, wenn :*
> *a. der Inhaber der Datensammlung dies ausdrücklich vorsieht und dafür eine zuständige Stelle bezeichnet hat;*
> *b. (…)*".

4.2 Anmeldung von Datensammlungen (Art. 3 und 4)

4.2.1 Anmeldung (Art. 3 Abs. 1, erster Satz und Abs. 2, zweiter Satz)

Bär&Karrer schlagen vor, Abs. 2 ganz zu streichen. Sie fragen sich, ob die Pflicht des Inhabers der Datensammlung, die Informationen nach Abs. 1 laufend zu aktualisieren beibehalten werden solle, wenn der Beauftragte nicht mehr gehalten ist, die erfolgten Änderungen periodisch zu erfassen.

4.2.2 Ausnahmen (Art. 4)

<u>Absatz 1</u>

Eine Organisation begrüsst die in Art. 4 Abs. 1 vorgesehenen Ausnahmen ausdrücklich (FER).

Fünf Organisationen und ein Privater verlangen, die Liste der Ausnahmen sei zu ergänzen bzw. an die in Artikel 18 vorgesehenen Ausnahmen für Bundesorgane an-

zugleichen (Datenschutzforum, santésuisse, swissbanking, swico, SVV und Belser). Swissbanking schlägt zudem vor, eine Ausnahme von der Meldepflicht dann vorzusehen, wenn die Transparenz der Bearbeitung gewährleistet ist, namentlich durch die Erfüllung der Informationspflicht nach dem neuen Art. 7a DSG oder wenn die Erkennbarkeit gemäss dem neuen Art. 4 Abs. 4 DSG gewährleistet ist. Bär&Karrer macht darauf aufmerksam, dass der geltende Art. 11 Abs. 3 Bst. b DSG im Rahmen der Revision des DSG nicht beibehalten wurde. Diese Bestimmung sieht *e contrario* vor, dass die privaten Inhaber der Datensammlungen nicht verpflichtet sind, ihre Datensammlungen anzumelden, wenn die Betroffenen von der Bearbeitung kenntnis haben. Nach Bär&Karrer wäre dieser Grundsatz in die Verordnung aufzunehmen.

Im Rahmen der Anhörung haben einige Stellung Nehmende Vorschläge zu Abs. 1 gemacht. Swissbanking und swico schlagen folgende Bestimmung vor:

"[1] Ausgenommen von der Pflicht zur Anmeldung der Datensammlungen sind die Datensammlungen nach Artikel 11a Absatz 5 Buchstaben a und c-f DSG sowie die folgenden Datensammlungen (Art. 11a Abs. 5 Bst. b DSG):

- *a. Datensammlungen mit Personendaten, über deren Bearbeitungszweck die betroffenen Personen gemäss art. 7a DSG informiert worden sind, oder denen sie ausdrücklich zugestimmt hat;*
- *b. Datensammlungen von Lieferanten oder Kunden, soweit sie keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile enthalten;*
- *c. Buchhaltungsunterlagen;*
- *d. Adressensammlungen, die ausschliesslich vom Inhaber der Datensammlung verwendet werden, soweit sie keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile enthalten;*
- *e. gleich wie Bst. b des Entwurfs;*
- *f. gleich wie Bst. c des Entwurfs;*
- *g. gleich wie Bst. d des Entwurfs;*
- *h. gleich wie Bst. e des Entwurfs."*

SVV und santésuisse schlagen vor, die Bestimmung analog Art. 18 Abs. 1 des Entwurfs zu fassen und Abs. 1 wie folgt zu formulieren:

"[1] Ausgenommen von der Pflicht zur Anmeldung der Datensammlungen sind die Datensammlungen nach Artikel 11a Absatz 5 Buchstaben a und c-f DSG sowie die folgenden Datensammlungen (Art. 11a Abs. 5 Bst. b DSG):

- *a. Adressensammlungen, soweit sie keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile enthalten und nur vom Inhaber der Adressensammlung verwendet werden;*
- *b. gleich wie der Entwurf;*
- *c. gleich wie der Entwurf;*
- *d. gleich wie der Entwurf;*
- *e. gleich wie der Entwurf;*
- *f. Datensammlungen von Geschäftspartnern oder Kunden, soweit sie keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile enthalte;*
- *g. Buchhaltungsunterlagen;*
- *h. Bibliothekdatensammlungen."*

Bär&Karrer schlagen vor, Art. 4 Abs. 1 um die folgenden Ausnahmen zu ergänzen:

"...

a. *Datensammlungen, von deren Bestand und Zweck die betroffenen Personen Kenntnis haben;*
b. *Datensammlungen mit besonders schützenswerten Personendaten oder Persönlichkeitsprofilen, von welchen der Inhaber bei der Ausübung seines Berufes, der die Kenntnis solcher Daten erfordert, erfahren hat. Variante : Datensammlungen, auf die der Inhaber bei der Ausübung seines Berufes angewiesen ist.*
c. *Datensammlungen über die eigenen Arbeitnehmer, wenn eine regelmässige Bekanntgabe nur aufgrund einer gesetzlichen Verpflichtung oder mit der Zustimmung der betroffenen Person erfolgt."*

Die konsultierten Kreise haben eine Reihe weiterer Bemerkungen zum Ausnahmekatalog von Abs. 1 formuliert.

Das Datenschutzforum fragt sich, ob ein Widerspruch zwischen Abs. 1 Bst. a und d entsteht, wenn Daten aus öffentlichen Verzeichnissen zur Kundenakquisition verwendet werden. Sind solche Datensammlungen zu melden, obwohl die Daten aus einer öffentlich zugänglichen Quelle stammen?

Für die Groupe Mutuel ist Bst. a zu stark eingeschränkt. Sie schlägt folgende Formulierung vor: "*… soweit sie nicht zu Zwecken verwendet werden, die Rechte der betroffenen Person gefährden*".

Bär&Karrer verlangt, die unter Bst. a vorgesehene Ausnahme sei nochmals zu prüfen. Die Anwaltskanzlei weist darauf hin, dass Adressdateien keine besonders schützenswerten Personendaten enthalten. Nach dem neuen Art. 11a Abs. 3 Bst. b DSG sind die Privaten gehalten, ihre Datensammlungen anzumelden, wenn sie regelmässig Personendaten an Dritte bekanntgeben. Bär&Karrer fragt sich, ob bei regelmässiger Bekanntgabe von Adressen an Dritte "es noch eine Rolle spielt, ob der Inhaber der Datensammlung diese selbst auch für Kundenakquisition verwendet".

Gemäss Belser wäre es falsch, zu glauben, dass nur die Nutzung der Daten für die Kundenakquisition die Rechte der Betroffenen bedrohen kann. Er schlägt vor, die Ausnahmen von Art. 19 des Entwurfs zu übernehmen.

Privatim ist der Auffassung, dass Abs. 1 Bst. a gleich wie Art. 18 Abs. 1 Bst. c formuliert werden sollte. Das Kriterium bei dessen Erfüllung eine Datensammlung angemeldet werden muss, sollte nicht die Nutzung zum Zweck der Kundenakquisition sein, sondern ob sie besonders schützenswerte Personendaten oder Persönlichkeitsprofile enthält und ob sie neben dem Versand von Korrespondenz auch noch anderen Zwecken dient.

Betreffend Abs. 1 Bst. b schlägt die Groupe Mutuel vor, den folgenden Teil zu streichen: "soweit ... verwendet werden und". Diese Änderung würde die Tragweite des Artikels nicht ändern, denn es handelt sich um Daten, die zu nicht personenbezogenen Zwecken verwendet werden.

Bär&Karrer ist der Auffassung, dass die Ausnahe von Abs. 1 Bst. c nicht nur die im Hinblick auf historische oder wissenschaftliche Nutzung archivierten Datensammlun-

gen umfassen sollte, sondern auch Daten, die für andere Zwecke aufbewahrt werden (z.B. in Erfüllung der Aufbewahrungspflicht nach Art. 962 OR).

Privatim hält Art. 4 Abs. 1 Bst. d für sachlogisch falsch, da es beim Register für Datensammlung um die Transparenz, nicht um den Rechtfertigungsgrund für die Führung der Datensammlung geht. Belser verlangt die Streichung dieser Bestimmung. Seiner Ansicht nach kann die Zustimmung der betroffenen Person nicht eine Ausnahme von der Meldepflicht rechtfertigen. Eine solche Ausnahme ist mit der ratio legis von Art. 11a Abs. 5 Bst. b DSG nicht vereinbar, insbesondere wenn es sich um Personendaten handelt, die auf Internet zugänglich sind.

Eine Organisation (swico) schlägt vor, eine Bestimmung vorzusehen, die den Beauftragten verpflichtet, ein Formular für die Anmeldung auf Internet zur Verfügung zu stellen.

Absatz 2

Fünf Organisationen verlangen – mit unterschiedlichen Begründungen – die Streichung von Abs. 2. Eine Organisation (Groupe Mutuel) vertritt die Auffassung, dass die Verpflichtung zur Führung einer Liste der der Meldepflicht unterliegenden Datensammlungen verbunden mit der Pflicht zur Führung einer zweiten Liste, welche die nicht meldepflichtigen Datensammlung umfasst einer Verpflichtung zur Führung einer Liste aller Datensammlungen gleichkommt. Dies würde einen unverhältnismässigen Aufwand erfordern und sei nicht mit der Zielsetzung der Meldepflicht nach DSG zu vereinbaren. Weitere Organisationen sind der Meinung, dass keine Rechtsgrundlage für die in Abs. 2 vorgesehene Verpflichtung besteht (swissbanking, swico, SVV, santésuisse). Zwei Organisationen sind der Auffassung, dass die Verpflichtung nach Abs. 2 weiter geht als das europäische Recht (swissbanking, swico).

Swico vertritt die Auffassung, die Formulierung "Liste der Datensammlungen, die nicht der Meldepflicht unterliegen" beziehe sich auf alle nicht meldepflichtigen Datensammlungen eines Unternehmens und nicht nur auch die Datensammlungen, die unter eine Ausnahmebestimmung fallen. Für den Fall der Beibehaltung von Abs. 2 schlägt swico eine neue Formulierung vor:

> *"[2] Der Inhaber der Datensammlung führt eine Liste der Datensammlungen nach Art. 11a Abs. 3 DSG, die nicht der Anmeldepflicht unterliegen. Diese Liste ist im Rahmen einer Abklärung gemäss Artikel 29 DSG dem Beauftragten zur Verfügung zu stellen."*

Swissbanking und swico sind im Übrigen der Ansicht, dass das in Abs. 2 vorgesehene Einsichtsrecht zu weit geht. Sie verlangen daher die Streichung dieser Bestimmung oder eventualiter eine Formulierung wie folgt:

> *"[2] Die Liste ist im Rahmen einer Abklärung gemäss Art. 29 DSG dem Beauftragten zur Verfügung zu stellen."*

Bär&Karrer ist der Auffassung, dass Abs. 2 keinen echten Mehrwert ergibt, was die Transparenz betrifft. Es wird daher die Streichung verlangt. Im Sinne einer Variante wird folgende Formulierung vorgeschlagen:

"[2] (….). Er teilt jeder betroffenen Person die Angaben zu den sie betreffenden Datensammlungen nach Art. 3 Abs. 1 auf Gesuch hin mit."

Swissbanking schlägt vor, in Art. 4 Abs. 2 folgendes zu präzisieren: "Reine Sicherungskopien, die lediglich der Gewährleistung der Integrität und der Verfügbarkeit von aktiv genutzten Datensammlungen dienen, sollen nicht separat registriert werden".

4.3 Bekanntgabe ins Ausland

4.3.1 Informationspflicht (Art. 5)

Belser hält den Titel von Art. 5 für verwirrlich, da Art. 7a DSG eine Informationspflicht der betroffenen Person vorsieht.

Zwei Organisationen sind der Auffassung, dass der *geltende Art. 5* nicht einfach gestrichen werden, sondern mutatis mutandis beibehalten werden sollte, da die dort vorgenommene Definition weiterhin einem Bedürfnis entspreche (swissbanking, swico).

Zwei Organisationen (Datenschutzforum, swico) sind der Auffassung, dem Beauftragten sollte eine klare Frist für die Prüfung der vorgelegten Garantien gesetzt werden. Der SGB ist der Ansicht, der Beauftragte sei zu informieren, *bevor* die Daten ins Ausland übermittelt werden, da eine nachträgliche Information den Schutz vor unzulässiger Datenbekanntgabe ins Ausland schmälert. Eine Organisation fragt sich, ob es nicht sinnvoll wäre, die Modalitäten der Informationspflicht genauer festzulegen (swico).

Bär&Karrer schlägt folgende Ergänzung von *Abs. 2* vor:

"*[2] Die Informationspflicht gilt nach erfolgter Information des Beauftragten als erfüllt für alle Bekanntgaben, die (…).*"

Zwei Organisationen äussern sich zu Abs. 2 Bst. b, zweiter Satzteil ("... solange die Datenschutzregeln unverändert bleiben"). Die erste (Datenschutzforum) fragt sich, ob es sich um eine zusätzliche Bedingung handle, die im formellen Gesetz hätte vorgesehen werden müssen. Die zweite (swico) ist der Auffassung, die Bedingung sei zu strikt und schlägt eine entsprechende Lockerung vor.

Eine Organisation (FER) stimmt dem Abs. 3 ausdrücklich zu. Bär&Karrer begrüsst diese Bestimmung ebenfalls, ist aber der Auffassung, dass die Pflicht zur Information des Beauftragten überflüssig ist, wenn Modellverträge verwendet werden. Es wird daher die Streichung vorgeschlagen. Zudem wird darauf hingewiesen, dass eine genügend lange Übergangsfrist zwischen der Publikation der Liste der Modellverträge und dem Inkrafttreten der Revision vorgesehen werden muss, damit die Unternehmen ihre Vertäge anpassen können. Swico vertritt die Auffassung, dass der Beauftragte nicht nur Modellverträge erarbeiten, sondern auch Modelle für Datenschutzregeln für die konzerninterne Übermitllung sowie Standardvertragsklauseln bereitstellen müsse. Diese Modelle müssten in Zusammenarbeit mit Berufsverbänden und Branchenorganisationen erarbeitet werden, in mehreren Sprachen zur Verfügung stehen und auf Internet veröffentlicht werden.

Eine Organisation (privatim) ist der Auffassung, dass es nicht nötig ist, in Abs. 4 vorzusehen, dass der Inhaber der Datensammlung angemessene Massnahmen ergreifen muss, um sicherzustellen, dass der Empfänger die Garantien und die Datenschutzregeln beachtet. Die Daten dürften ohnehin nur dann ins Ausland bekanntgegeben werden, wenn ihr Schutz gewärleistet sei. Bär&Karrer stellt sich die Frage, ob die Bestimmung nicht die Kompetenz des Bundesrates zur Regelung der Einzelheiten der Informationspflicht überschreitet und hält weiter fest, der Inhalt von Abs. 4 entspreche nicht dem Titel des Art. 5.

4.3.2 Liste der Staaten mit angemessener Datenschutzgesetzgebung (Art. 7)

Privatim und swissbanking sind der Auffassung, dass die Liste des Beauftragten betreffend die Staaten, die über eine Gesetzgebung verfügen, die ein angemessenes Datenschutzniveau verfügen, verbindlichen Charakter haben müsse. Für privatim muss der Beauftragte ausdrücklich zur Publikation dieser Liste verpflichtet werden.

4.4 Allgemeine technische und organisatorische Massnahmen (Art. 8 Abs. 1, erster Satz und Abs. 4)

Die angehörten Kreise haben zu der vorliegenden Bestimmung keine Bemerkungen vorgebracht.

Eine Organisation (swico) schlägt im vorliegenden Zusammenhang eine Änderung bei Art. 4 Abs. 1 Bst. d vor (vgl. Ziff. 4.2.2).

4.5 Bearbeitungsreglement (Art. 11)

Eine Organisation (Datenschutzforum) begrüsst die Tatsache, dass der Inhalt des Reglements genauer umschrieben wird.

Bär&Karrer schlägt vor, nicht nur auf Art. 11a Abs. 3, sondern auch auf dessen Abs. 5 zu verweisen. Weiter wird davon ausgegangen, dass der Inhaber der Datensammlung nur dann verpflichtet werden sollte, ein Bearbeitungsreglement zu erstellen, wenn der Grundsatz der Transparenz dies verlangt. Es wird daher folgende Änderung vorgeschlagen: "*Soweit es der Grundsatz der Transparenz erforderlich macht, erstellt der Inhaber einer meldepflichtigen automatisierten Datensammlung (Art. 11a Abs. 3 und 5 DSG) ein Bearbeitungsreglement, das insbesonsere (…)*". Es wird schliesslich vorgeschlagen, "automatisierte Datensammlung" durch "Datensammlung" zu ersetzen.

Gemäss Privatim ist ein Bearbeitungsreglement für alle Datensammlungen nach Art. 11a Abs. 3 DSG zu erstellen. Das Kriterium der Meldeflicht sei aus datenschutzrechtlicher Sicht nicht entscheidend. Würde ein Unternehmen über einen Datenschutzverantwortlichen verfügen, so gäbe es gerade keine Meldepflicht, weshalb ihm auch kein Bearbeitungsreglement zur Verfügung zu stellen wäre.

Um den Rahmenbedingungen der KMU besser Rechnung zu tragen, schlägt eine Organisation (SDV) vor, in Abs. 1 zu präzisieren, dass das Reglement namentlich die "funktionelle Unabhängigkeit der Personen garantiert, die die Funktionen des Datenschutzbeauftragten wahrnehmen".

Belser ist der Ansicht, dass Abs. 2, 2. Satz, gestrichen werden kann, da die entsprechende Verpflichtung bereits in Art. 12b Abs. 2 Bst. c des Entwurfs vorgesehen sei.

4.6 Datenschutzberater (5. Abschnitt)

4.6.1 Bezeichnung und Mitteilung an den Beauftragten (Art. 12a)

Fünf Organisationen und ein Privater sprechen sich gegen die in der deutschen Fassung in der Verordnung eingeführte Bezeichnung – "Datenschutzberater" statt "Datenschutzverantwortlicher" – aus (SGS, Datenschutzforum, privatim, RVK, SVV, Belser). Eine Organisation stimmt dieser Lösung ausdrücklich zu (swico).

Die Groupe Mutuel schlägt vor zu präzisieren, dass der Datenschutzberater die Anforderungen von Art. 12a *Abs. 2* und 12b erfüllen muss.

Eine Organisation (SGS) fragt sich, "in wiefern die Unabhängigkeit der Datenschutzberaters gegeben ist, wenn keine Meldung an den Eidg. Datenschutz- und Öffentlichkeitsbeauftragten verlangt wird".

Zwei Organisationen (RVK, FER) begrüssen die Tatsache, dass der Datenschutzberater sowohl ein Mitarbeiter des Inhabers der Datensammlung als auch ein Dritter sein kann (Art. 12a Abs. 2). Die IVSK begrüsst, dass der Datenschutzberater als Funktion definiert wird.

Der SDV hält fest, dass die Anforderung einer vollständigen organisationellen Unabhängigkeit des Datenschutzberaters für die KMU Probleme bereiten könnte. Die Tatsache, dass diese Funktion unter mehreren Personen aufgeteilt werden könne, sei somit zu begrüssen. Diese Möglichkeit sollte jedoch ausdrücklich in der Verordnung vorgesehen werden, nicht nur im Kommentar. Um den Rahmenbedingungen von KMU besser Rechnung zu tragen, schlägt der SDV ferner vor, den Abs. 2 der vorliegenden Bestimmung folgendermassen zu formulieren:

> *"[2] Der Inhaber der Datensammlung kann einen oder mehrere Mitarbeiter oder einen Dritten als Datenschutzberater bezeichnen. In ihrer Funktion als Datenschutzberater sind diese Personen organisatorisch dem Inhaber der Datensammlung direkt unterstellt und müssen über die erforderlichen Fachkenntnisse verfügen."*

Das Datenschutzforum fragt sich, wer die Einhaltung der in Abs. 2, 2. Satz, festgehaltenen Anforderung (Verbot der Ausübung von Tätigkeiten, die mit den Aufgaben des Datenschutzberaters nicht vereinbar sind) überprüfen wird.

Drei Organisationen (SGS, RVK, Datenschutzforum) sind der Ansicht, es wäre angezeigt, die Anforderungen an die Ausbildung des Datenschutzberaters zu präzisieren.

4.6.2 Aufgaben und Stellung des Datenschutzberaters (Art. 12b)

Zwei Organisationen (swissbanking, swico) weisen darauf hin, dass Abs. 1 Bst. a so verstanden werden könnte, dass sich die Zuständigkeit des Datenschutzverantwortlichen bloss auf Datensammlungen beschränkt und somit nicht den datenschutzkonformen Umgang mit personenbezogenen Daten im Unternehmen allgemein umfasst.

Swissbanking ist der Auffassung, dass Abs. 1 Bst. b nicht jeder Person ein Recht auf Einsicht in die vom Inhaber der Datensammlung geführten Liste der Datensammlungen zugestehen soll. Daher wird folgende Neuformulierung vorgeschlagen:

"b. Er führt eine Liste der Datensammlungen des Inhabers der Datensammlungen nach Art. 11a Abs. 3 DSG und er stellt diese auf Gesuch hin dem Beauftragten im Rahmen von Abklärungen gemäss Art. 29 Abs. 2 DSG zur Verfügung."

Swico und der SVV sind ebenfalls der Ansicht, das Recht, die Liste der vom Inhaber der Datensammlung geführten Liste zu konsultieren sei zu breit gefasst. Sie schlagen daher Streichung oder Einschränkung dieser Bestimmung vor. Bär&Karrer empfiehlt, "oder anderen Personen" durch *"oder betroffenen Personen, soweit sie betreffend, (…)"* zu ersetzen.

Um den Rahmenbedingungen der KMU besser Rechnung zu tragen, schlägt der SDV vor, den Abs. 1 mit der folgenden Bestimmung zu ergänzen:

"...*er dokumentiert und überprüft regelmässig alle technischen und organisatorischen Massnahmen zur Sicherung der Datensammlungen.*"

Betreffend Abs. 2 Bst. a ist swissbanking der Ansicht, die Unabhängigkeit des Datenschutzberaters sei zu relativieren. Sie sei beschränkt, weil dieser nur Empfehlungen aussprechen könne und der Inhaber der Datensammlung zuständig sei, um Entscheidungen zu treffen.

Swico schlägt vor, in der revidierten VDSG sei die fachliche Selbständigkeit und Unabhängigkeit des Datenschutzberaters besonders hervorzuheben und schlägt vor, Abs. 2 Bst. a wie folgt zu formulieren::

"a. Er übt seine Funktion fachlich selbständig und unabhängig aus, ohne diesbezüglichen Weisungen des Inhabers der Datensammlung zu unterliegen."

Eine Organisation (RVK) ist der Ansicht, dass Abs. 2 Bst. b überflüssig ist, weil die Frage der Ressourcen in den Zuständigkeitsbereich des Inhabers der Datensammlung fällt. Es könnten indessen zu diesem Punkt Richtwerte in einem Anhang vorgesehen werden. Die SGS schlägt ebenfalls vor, die erforderlichen Ressourcen sollten im Anhang oder allenfalls einer Richtlinie des Beauftragten festgelegt werden. Das Datenschutzforum macht einen analogen Vorschlag.

Für privatim müsste in der Verordnung (und nicht bloss in den Erläuterungen) festgehalten werden, dass gegen den Datenschutzverantwortlichen keine Massnahmen mit Sanktionscharakter wegen der Erfüllung seiner Aufgaben ergriffen werden dürfen. Beispielsweise wäre ein Kündigungsschutz vorzusehen. Ausserdem sei eine Pflicht zur Zusammenarbeit mit dem EDÖB vorzusehen und der Datenschutzverantwortliche gegenüber dem EDÖB von beruflichen oder anderen Schweigepflichten zu befreien.

4.7 Ausnahmen von der Anmeldepflicht, Bundesorgane (Art. 18)

Die Groupe Mutuel ist der Auffassung, Abs. 3 sei überflüssig, aus denselben Gründen, wie sie beim Art. 4 Abs. 2 angeführt wurden (vgl. Ziff 4.2.2).

4.8 Bekanntgabe ins Ausland, Bundesorgane (Art. 19)

Die FER begrüsst, dass für die Bundesorgane die gleichen Regeln gelten sollen wie für die Privaten.

4.9 Datenschutzberater, Bundesorgane (Art. 23)

Privatim verlangt die Streichung von Abs. 3. Die Bundesorgane müssen direkten Kontakt zum Beauftragten haben.

4.10 Verfahren bei der Bewilligung von Pilotversuchen (Art. 26a)

Privatim schlägt vor, die Bestimmung dahingehend zu ändern, dass der Bundesrat seinen Entscheid begründen muss, wenn er die Stellungnahme des Beauftragten nicht berücksichtigt.

4.11 Register der Datensammlungen, Bundesorgane (Art. 28)

Belser ist der Auffassung, dass Abs. 4 nicht nur unnötig, sondern auch falsch ist. Die Folgen einer Verletzung der Meldepflicht seien schon in Art. 34 Abs. 2 Bst. a DSG geregelt. Die Reaktion des EDÖB müsste deshalb sein, den fehlbaren Inhaber einer meldepflichtigen Datensammlung bei den Strafjustizbehörden anzuzeigen.

4.12 Eidg. Datenschutz- und Öffentlichkeitsbeauftragter, Sitz und Rechtsstellung (Art. 30 Abs. 2 und 3)

Eine Organisation (privatim) fordert, es sei festzuhalten, dass der EDÖB auf eine feste Amtstdauer (mind. 4 Jahre) gewählt wird. Zudem sei zu erwähnen, dass der EDÖB über die notwendigen Fachkompetenzen zu verfügen hat und keine Nebenerwerbstätigkeit ausüben darf, die zu Interessenkonflikten führen kann. Des weiteren seien die personal- und finanzrechtlichen Kompetenzen des EDÖB zu umschreiben (analog, wie dies für den Departementsvorsteher der Fall ist). Schliesslich sei der Budgetprozess eigenständig auszugestalten; der Bundesrat ist zu verpflichten, das Budget des EDÖB unverändert zu übernehmen.

4.13 Beziehungen zu anderen Behörden und privaten Personen (Art. 31 Abs. 1)

Privatim ist der Ansicht, dass diese Bestimmung wie eine Unterstellung des Beauftragten unter die Bundeskanzlei wirkt. Der Beauftragte müsse direkt mit dem Bundesrat verkehren können.

4.14 Gebühren (Art. 33 Abs. 1)

Privatim und swissbanking halten fest, dass der Beauftragte über genügend Mittel verfügen muss, um Gutachten zu erstellen und dass er die Praxis hinsichtlich der Gebühren rechtzeitig und klar bekanntgeben muss.

4.15 Weitere Bemerkungen

Im Folgenden sind die Bemerkungen der Angehörten zusammengestellt, die sich auf den Entwurf als Ganzes beziehen oder einzelne Artikel betreffen, die nach dem Entwurf nicht Gegenstand einer Revision sind:

- Die Verordnung sollte mit einer Bestimmung ergänzt werden, welche die Anforderungen an die Erkennbarkeit der Bearbeitung (Art. 4 Abs. 4 DSG) konkretisiert (swico).

- Die Unabhängigkeit des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) ist nicht vollständig gewährleistet. Dies ist auf Verordnungsstufe nachzuholen (privatim).
- Der neue Art. 10a DSG gilt sowohl für den privaten wie den öffentlichen Bereich. Daher wäre es angezeigt, auch Art. 1 Abs. 6 VDSG entsprechend anzupassen (swissbanking, swico).
- Art. 1 Abs. 7 VDSG sollte dahingehend ergänzt werden, dass eine gesetzliche Geheimhaltungspflicht ebenfalls ein Grund für eine Einschränkung der Auskunft über Personendaten einer verstorbenen Person darstellen kann (swissbanking). Der swico schlägt vor, dass auch die gesetzlichen oder eingesetzten Erben als auskunftsberechtigt anerkannt werden sollten.
- Die Angemessenheit von Massnahmen zur Gewährleistung der Datensicherheit nach Art. 8 Abs. 2 Bst. d sollte auch den personellen, technischen und finanziellen Aufwand umfassen, wie dies ausdrücklich in Art. 17 Abs. 1, 2. Satz, der EU-Datenschutzrichtlinie 95/46/EG vorgesehen ist (swico).

5. Beurteilung des Entwurfs zu einer Verordnung über die Datenschutzzertifizierungen

5.1 Allgemeine Bemerkungen

5.1.1 Allgemeine Würdigung des Enwurfs

Eine Bundesbehörde (EKK) und 3 Organisationen (acsi, kf, SDV) stimmen dem Entwurf ausdrücklich zu.

5 Organisationen äussern sich skeptisch (CP, FER, CVAM, IVSK, swico). Die Vorlage sei schwer verständlich und sehr technisch formuliert (CP, CVAM). Die FER ist der Ansicht, die vorgesehenen Voraussetzungen für eine Zertifizierung bedeuteten einen administrativen Aufwand, der, im Vergleich zum damit verbundenen Vorteil, kaum verhältnismässig sei (ähnlich auch swico). Die mit der Zertifizierung verbundenen Kosten seien für KMU wahrscheinlich prohibitiv. Auch die IVSK stellt sich die Frage nach dem Mehrwert der Zertifizierung. Die Einhaltung der rechtlichen Anforderungen sei an sich eine Selbstverständlichkeit. Das systematische Angehen des Datenschutzes und die Schulung der Mitarbeitenden stellten indessen tatsächlich einen Mehrwert dar. Die swico äussert sich positiv gegenüber der Datenschutzzertifizierung von Produkten. Diese wird den Einsatz von datenschutzgerechten informationstechnologischen Produkten fördern und damit längerfristig eine allgemeine Hebung des Datenschutzniveaus bewirken.

Eine Behörde (SAS) und 3 Organisationen (Datenschutzforum, privatim, SGS) sprechen sich gegen den Entwurf aus. Für die SAS ist nicht akzeptabel, dass die Vorlage kein offizielles Datenschutz-Qualitätszeichen (DSQ) vorsieht. Eine Organisation vertritt die Auffassung, das Zertifizierungsverfahren sei in der vorgeschlagenen Form untauglich (privatim). Nur eine unabhängige Stelle könne eine unabhängige Zertifizierung gewährleisten, daher müsse der EDÖB selbst die Zertifizierungen vergeben oder zumindest eine verbindliche Kontrolle der Prüfberichte vornehmen. Das Datenschutzforum und die SGS sind der Ansicht, dass der Entwurf die Mindestanforderungen an die Zertifizierung nicht klar regelt (so auch die RVK, ohne indessen die Vorlage ausdrücklich abzulehnen). Die von einer Arbeitsgruppe unter Leitung des EDÖB entworfene konkretisierende Regelung hätte die notwendige Klarheit geschaffen.

Die übrigen Stellungnahmen äussern sich nicht zum Entwurf in seiner Gesamtheit.

5.1.2 Verzicht auf ein offizielles Datenschutz-Qualitätszeichen

Mehrere Stellungnahmen halten ausdrücklich fest, dass sie der mit dem Entwurf vorgesehenen Lösung – Regelung der Minimalanforderungen und Verzicht auf ein offizielles DSQ – zustimmen oder diese begrüssen (EKK, acsi, CP, CVAM, FER, kf, Belser).

Zwei Behörden (EDÖB, SAS) und drei Organisationen (Datenschutzforum, RVK, SGS) verlangen, die Verordnung solle ein offizielles DSQ vorsehen. Begründet wird dies damit, dass so, namentlich aus der Sicht der Konsumentinnen und Konsumenten, mehr Transparenz geschaffen würde und negative Auswirkungen, wie sie in anderen Bereichen auftreten, vermieden werden könnten.

5.2 Zertifizierungsstellen (1. Abschnitt)

5.2.1 Anforderungen (Art. 1)

Drei Organisationen und ein Privater äusserten sich zu den Mindestanforderungen an die Qualifikation des Personals, welches Zertifizierungen durchführt (Abs. 5 und Anhang).

Das Datenschutzforum, die RVK und die SGS begrüssten ausdrücklich, dass hohe Anforderungen an die Qualifikation des Personals aufgestellt werden. Es sei indessen darauf zu achten, dass diese Vorschriften einheitlich ausgelegt werden; der Praxisnachweis müsse streng überprüft werden (Datenschutzforum, SGS). Zudem sollte auch Auditerfahrung gefordert werden, eine entsprechende Ausbildung allein genügt nicht (SGS). Allenfalls könnte vorgesehen werden, dass die Auditorinnen und Auditoren gemeldet werden müssen (Datenschutzforum). Die RVK schlägt zudem vor, die Voraussetzungen der praktischen Tätigkeit und der Ausbildung im Bereich des Datenschutzes bzw. der Informationssicherheit kumulativ statt alternativ zu fordern.

Belser hält die Anforderungen an die Qualifikation des Pesonals für zu tief angesetzt.

5.2.2 Akkreditierungsverfahren (Art. 2)

Die Organisation privatim bemängelt, dass materielle Bestimmungen darüber fehlen, mit welchem Ziel und mit welchen Kompetenzen der Beizug des EDÖB erfolgt. Es sollte ihm ein Mitentscheidungsrecht bei der Akkreditierung zukommen.

Die swico schlägt vor, den Beizug des EDÖB nicht nur für das Akkreditierungsverfahren und die Nachkontrolle, sondern auch für die Suspendierung und den Widerruf der Akkreditierung ausdrücklich vorzusehen.

5.2.3 Ausländische Zertifizierungsstellen (Art. 3)

Der EDÖB vertritt die Auffassung, dass das DSG ihm keinerlei Verfügungsbefugnis überträgt und dass auf Verordnungsebene eine solche – auch eine beschränkte – nicht eingeführt werden könne. Der Entscheid über die Anerkennung wäre daher der SAS oder dem Bundesamt für Justiz zu übertragen; zuvor wäre der EDÖB zu konsultieren.

Für die SGS ist nicht nachvollziehbar, weshalb ein eigener Artikel betreffend ausländische Zertifizierungsstellen vorgesehen wird. Die Organisation ist der Auffassung, die Akkreditierungsanforderungen seien bereits genügend klar geregelt.

5.3 Gegenstand und Verfahren (2. Abschnitt)

5.3.1 Zertifizierung von Organisation und Verfahren (Art. 4)

Der EDÖB und 5 Organisationen (Datenschutzforum, SGS, swico, FER, privatim) äusserten sich zum Absatz 3, der die Mindestanforderungen an ein Datenschutzmanagementsystem (DSMS) festlegt. In ihren Stellungnahmen vertraten sie die Ansicht, der Verweis auf die Norm ISO 27001: 2005 genüge nicht.

Primär wurde darauf hingewiesen, dass es bei der Datenschutzzertifizierung nicht nur um die Informationssicherheit gehen dürfe, sondern dass es darum gehen müsse, die Datenschutzgrundsätze korrekt umzusetzen (Datenschutzforum, SGS). Die erwähnte ISO-Norm enthalte diesbezüglich keine konkreten Anforderungen, zudem trügen auch die in Absatz 2 aufgeführten Voraussetzungen für ein DSMS wenig zur korrekten Umsetzung der Datenschutzgrundsätze bei (swico). Der EDÖB verlangt, die Befugnis zu erhalten, Richtlinien zu erlassen, wie dies für die Produktezertifizierung der Fall ist (vgl. Art. 5 Abs. 3). Privatim partage la même opinion que le préposé.

Weiter wurde festgehalten, dass bei der Zertifizierung von Organisation und Verfahren auch Qualitätsmanagementsysteme eine bedeutende Rolle spielen, weshalb gleichwertig auch auf ISO 9001 zu verweisen sei (privatim, Belser).

Die FER betrachtet die Bestimmung von Artikel 4 Absatz 3 als nicht genügend klar. Ein Unternehmen, das eine Zertifikation erlangen will, kann die dafür zu erfüllenden Anforderungen nur ersehen, wenn es sich die ISO-Norm beschafft oder den erläuternden Bericht zur Verordnung liest. Die Anforderungen sind zudem zu stark einschränkend, so dass das Zertifizierungsverfahren toter Buchstabe zu bleiben droht.

5.3.2 Zertifizierung von Produkten (Art. 5)

Lediglich der swico äusserte sich zur vorliegenden Bestimmung. Sie konnte bezüglich Umschreibung der zertifizierbaren Produkte (Abs. 1) nicht nachvollziehen, weshalb eine Beschränkung auf "Softwareprodukte oder deren Kombination mit bestimmten Hardwareprodukten" erfolgt. Die schleswig-holsteinische Datenschutz-Auditverordnung definiert dem gegenüber die zertifizierbaren informationstechnologischen Produkte viel allgemeiner als "Hardware, Software und automatisierte Verfahren".

Zu den Prüfungskriterien (Abs. 2) hielt die swico fest, dass die dort formulierten Anforderungen von den meisten Produkten erfüllt werden dürften. Wirklich datenschutzfördernd wäre dagegen die durch das zu zertifizierende System unterstützte Wahrung des Zweckbindungsgebots, die automatisierte Kontrolle bzw. Beschränkung der Verknüpfung von Elementen einer Datenbank, die systemgestützte Kontrolle der Bekanntgabe von Personendaten an Dritte, die Unterstützung des Anwenders bei der Erfüllung der Auskunftspflichtsowie Funktionen zur Umsetzung von Löschungs- und Berichtigungsansprüchen.

5.3.3 Erteilung und Gültigkeit der Datenschutzzertifizierung (Art. 6)

Eine Organisation verlangt ein anderes System der Erteilung der Zertifizierung (privatim). Die Bestimmung sollte vorsehen, dass die Berichte dem EDÖB vorgelegt werden, der entweder ein offizielles DSQ vergibt (vgl. Ziff. 5.1.1) oder zumindest die Berichte materiell überprüft (ähnlich auch swico, vgl. Ziff. 5.3.4). Dafür wären ihm entsprechende Ressourcen zur Verfügung zu stellen. Gegen diese Lösung spricht sich ausdrücklich U. Belser aus.

Der swico weist darauf hin, dass in *Absatz 1* auch die durch die Artikel 4 und 5 aufgestellten Anforderungen erwähnt werden sollten.

Zu *Absatz 2* hält die FER fest, dass das Erfordernis einer jährliche Überprüfung im Verhältnis zur Gültigkeitsdauer von 3 Jahren exzessiv sei.

Der swico bemerkt zu *Absatz 3*, dass die Bestimmung in der Praxis zu erheblichen Problemen führen könnte, wenn sie so verstanden würde, dass die Zertifizierung für jede neue Auflage eines Softwarepakets wiederholt werden muss. Dies wäre mit einem sehr grossen Aufwand verbunden.

5.3.4 Mitteilung des Ergebnisses des Zertifizierungsverfahrens (Art. 8)

Zu *Absatz 1* hält die swico fest, dass nicht die zertifizierte Stelle, sondern die Zertifizierungsstelle dem EDÖB die Ergebnisse mitteilen sollte. Der EDÖB muss über sämtlich von den Zertifizierungsstellen vergebenen DSQ unterrichtet werden, sonst droht ein Wildwuchs bei der Vergabe der DSQ.

Zu *Absatz 2* schlägt die swico eine Änderung vor. Wenn die Zertifizierungsstelle bei ihrer Kontrolltätigkeit (Art. 6 Abs. 2) feststellt, dass die Zertifizierungsvoraussetzungen sich geändert haben, dann hat in jedem Fall die Zertifizierungsstelle den EDÖB zu informieren. Sonst wird die Umsetzung der Ergebnisse der Nachkontrollen dem Ermessen der zertifizierten Stellen anheim gestellt. Dem EDÖB soll die Möglichkeit eingeräumt werden, die ihm gemeldeten Bewertungsberichte und Zertifizierungsdokumente zu prüfen und gegebenenfalls dazu Empfehlungen abzugeben. Die DSQ sollen von den Zertifizierungsstellen erst ausgegeben werden dürfen, wenn die Bewertungsberichte und die Zertifizierungsunterlagen durch den EDÖB im Hinblick auf die Einhaltung der Datenschutzvorschriften geprüft worden sind.

Die FER verlangt die Streichung von Absatz 2. Die Zertifizierungsstelle als Vertragspartner des zertifizierten Unternehmens soll dieses nicht beim EDÖB "denunzieren" müssen. Diesbezüglich sollte dieselbe Lösung getroffen werden wie für den betrieblichen Datenschutzberater (Art. 12b E-revVDSG). Das zertifizierte Unternehmen sollte generell nicht der Aufsicht zweier Stellen (Zertifizierungsstelle und EDÖB) unterliegen.

Der swico schlägt betreffend *Absatz 3* eine Erweiterung vor: Zertifizierungsberichte und Bewertungsunterlagen sollten nicht lediglich dem EDÖB mitgeteilt werden, sondern in vollständiger oder zusammengefasster Form online allgemein zugänglich gemacht werden. Jede interessierte Person sollte die Möglichkeit haben, vom EDÖB eine Kopie eines Bewertungsberichts oder der Zertifizierungsunterlagen zu verlangen.

5.4 Sanktionen (3. Abschnitt)

5.4.1 Sisitierung und Entzug der Zertifizierung (Art. 9)

Der swico schlägt zu dieser Bestimmung zwei Änderungen vor:

- *Absatz 1*: Beifügen, dass die Zertifizierungsstelle vor Entzug oder Sistierung einer Zertifizierung eine Stellungnahme des Beauftragten einholt.
- *Absatz 3*: Letzten Teilsatz streichen, da verlangt wird, es seien alle Zertifizierungen zu melden (vgl. oben, Ziff. 5.3.4).

5.4.2 Verfahren bei Aufsichtsmassnahmen der oder des Beauftragten (Art. 10)

Die EKK begrüsst diese Bestimmung und betont, dass der Staat bei schweren Mängeln eingreifen können muss. Der EDÖB sei für die Erfüllung dieser neuen Aufgabe mit den notwendigen Ressourcen auszustatten.

Der swico schlägt einen neuen Absatz 5 vor. Es soll ausdrücklich vorgesehen werden, dass die Aufsichtskompetenzen des EDÖB sich auch auf den Fall beziehen, dass er Mängel bei der Zertifizierungsstelle feststellt. Der letzte Satz von Absatz 4 sollte daher in einen separaten Absatz aufgenommen und verdeutlicht bzw. erweitert werden.

5.5. Weitere Bemerkungen

Im Folgenden sind die Bemerkungen der Angehörten zusammengestellt, die sich auf den Entwurf als Ganzes beziehen oder Punkte betreffen, die im Entwurf nicht vorgesehen sind:

- Für bestimmte Bereiche (z.B. Outsourcing der Datenbearbeitung, gewisse Datenbearbeitungen im Gesundheitswesen) wäre ein Zertifizierungsverfahren zwingend vorzuschreiben (privatim).
- Um die Markttransparenz zu fördern, ist es notwendig, dass der EDÖB eine Liste der Qualitätszeichen im Bereich des Datenschutzes führt (EKK).
- Das grundlegende Problem ist, dass eine internationale Anerkennung der Datenschutzzertifizierung fehlt (swico).
- Betont wird auch, dass die Zertifizierung freiwillig sein muss (FER, swico).

Anhörung zum Entwurf zu einer Änderung der Verordnung zum Bundesgesetz über den Datenschutz (VDSG, 235.11) und zu einer Verordnung über die Datenschutzzertifizierungen

Liste der Anhörungsadressaten / Liste des destinataires / Lista dei destinatari

1. Dachverbände der Wirtschaft / Associations faîtières de l'économie / Federazioni centrali dell'economia (11)

- economiesuisse
  Verband der Schweizer Unternehmer
  Hegibachstrasse 47
  Postfach
  8032 Zürich

- Schweizerischer Arbeitgeberverband
  Hegibachstrasse 47
  Postfach
  8032 Zürich

- Schweizerische Bankiervereinigung
  swissbanking
  Aeschenplatz 7
  Postfach 4182
  4002 Basel

- Travail Suisse
  Postfach 5775
  3001 Bern

- Schweiz. Kaufmännischer Verband (SKV)
  Hans Huber-Strasse 4
  Postfach 687
  8027 Zürich

- Fédération des entreprises romandes (FER)
  98, rue de Saint-Jean
  Case postale 5278
  1211 Genève 11

- Schweizerischer Gewerbeverband (SGV)
  Schwarztorstrasse 26
  3001 Bern

- Schweiz. Bauernverband (SBV)
  Haus der Schweizer Bauern
  Laurstrasse 10
  5201 Brugg

- Schweiz. Gewerkschaftsbund (SGB)
  Monbijoustrasse 61
  Postfach 64
  3000 Bern 23

- Schweiz. Versicherungsverband SVV
  C.F. Meyer-Strasse 14
  Postfach 4288
  8022 Zürich

- santésuisse
  Römerstrasse 20
  4502 Solothurn

2. Weitere Organisationen und Verbände / Autres organisations et associations / Altre organizzazioni e associazioni (35)

- Associazione consumatrici della Svizzera italiana
  Via Lambertenghi 4
  6900 Lugano

- Wissenschaftliche Vereinigung zur Pflege des Wirtschafts- und Konsumentenschutzrechts (VKR)
  Toblerstr. 97/Neuhausstr. 4
  Postfach 763
  8044 Zürich

- Stiftung für Konsumentenschutz (SKS)
  Monbijoustrasse 61
  Postfach
  3000 Bern 23

- Konsumentenforum Schweiz (KF)
  Grossmannstrasse 29
  Postfach 294
  8037 Zürich

- Fédération romande des consommateurs
  Rue de Genève 7
  Case postale 6151
  1002 Lausanne

- Schweizer Direktmarketing Verband (SDV)
  Postfach 616
  8501 Frauenfeld

- Schweiz. Anwaltsverband
  Marktgasse 4
  Postfach 8321
  3001 Bern

- Schweizerischer Juristenverein
  Postfach 1954
  4001 Basel

- Schweiz. Verband Creditreform (SVC)
  Teufenerstr.36
  9000 St. Gallen

- Verband Schweiz. Kreditbanken und Finanzierungsinstitute
  Toblerstr. 97 / Neuhausstr. 4
  8023 Zürich

- Schweiz. Adressen- und Werbezentrale (AWZ)
  Hirschengraben 7
  3001 Bern

- Verband von Wirtschaftsauskunfteien in der Schweiz (VWA)
  c/o Dun & Bradstreet (Schweiz) AG
  In der Luberzen 1
  8902 Urdorf

- Fédération suisse des journalistes (FSJ)
  Grand-Places 14a
  Case postale 316
  1701 Fribourg

- Schweizerischer Buchhändler- und Verleger-Verband (SBVV)
  Alderstr. 40
  Postfach
  8034 Zürich

- Swiss Mail, die Private Post Vertragungsorganisationen
  Birsigstr. 79
  4054 Basel

- La Poste suisse
  Viktoriastr. 21
  3030 Bern

- ICTswitzerland
  Postfach 515
  Kramgasse 5
  3000 Bern 8

- CLUSIS
  Association suisse de la sécurité des systèmes d'information
  Case postale 9
  CH 1000 Lausanne 26

- DSB+CPD. CH
  c/o B. Baeriswyl
  Datenschutzbeauftragter des Kantons Zürich
  Postfach
  8090 Zürich

- Ausgleichskasse EXFOUR
  Vereinigung der Verbandsausgleichskassen
  Postfach
  4010 Basel

- SUVA
  Schweiz. Unfallversicherungsanstalt
  Fluhmattstrasse 1
  6004 Luzern

- Vereinigung der Kantonsärzte der Schweiz
  Dr. med. H. Binz
  Präsident
  Gesundheitsamt
  Ambassadorenhof
  4509 Solothurn

- Schweizerische Patienten-Organisation
  Postfach
  8023 Zürich

- Verband Schweizerischer Inkasso-treuhandinstitute
  Dr. iur. Robert Simmen
  Toblerstrasse 97
  Postfach 382
  8044 Zürich

- Schweizer Werbung (SW)
  Kappelergasse 14
  Postfach 4675
  8022 Zürich

- Information Systems audit and control association (ISACA)
  c/o Daniela S. Gschwend
  Swiss Re
  Mythenquai 50/60
  8022 Zürich

- Konferenz der kantonalen Ausgleichskassen
  Chutzenstr. 10
  3007 Bern

- IV-Stellen-Konferenz (IVSK)
  Geschäftsstelle IVSK
  Landenbergstrasse 35
  6005 Luzern

- ASIP
  Schweiz. Pensionskassenverband
  Herrn Walser
  Talstrasse 20
  8001 Zürich

- FMH Verbindung der Schweizer Aerzte (FMH) Generalsekretariat
  Elfenstrasse 18
  Postfach 293
  3000 Bern 16

- Schweizerische Gesellschaft für Mikrobiologie
  Sonnenrain 10
  3150 Schwarzenburg

- Schweizerische Gesellschaft für Prävention und Gesundheitswesen
  Zentralsekretariat
  Effingerstrasse 54
  Postfach 8172
  3001 Bern

- Datenschutz-Forum
  Frau Ursula Uttinger, Präsidentin
  Hotzestrasse 35
  8006 Zürich

- Verein Unternehmensdatenschutz
  Jacques Beglinger, RA
  Rämistr. 7
  Postfach 519
  8024 Zürich

- Schweizerischer Wirtschaftsverband der Informations-, Kommunikations- und Organisationstechnik (swico)
  Technoparkstrasse 1
  8005 Zürich

-

Anhörung zum Entwurf zu einer Änderung der Verordnung zum Bundesgesetz über den Datenschutz (VDSG, 235.11) und zu einer Verordnung über die Datenschutzzertifizierungen

Anhörungsadressaten und weitere Organisationen, welche Stellungnahmen eingereicht haben

---

1. Anhörungsadressaten, welche geantwortet haben (32)

1.1 Organisationen (22)

ACSI	Associazione Consumatrici della Svizzera Italiana Stabile amministrativo 6932 Breganzona
CVAM	Chambre vaudoise des arts et métiers Case postale 1215 1001 Lausanne
CP	Centre patronal Rue du lac 2 1094 Paudex
Datenschutz-forum	Datenschutzforum Schweiz c/o Ursula Uttinger Hotzestr. 35 8006 Zürich
Die Post La Poste La Posta	Die Schweizerische Post La Poste Suisse La Posta Svizzera Viktoriastr. 21 3030 Bern
FER	Fédération des entreprises romandes 98, rue de Saint-Jean Case postale 5278 1211 Genève 11
FRC	Fédération romande des consommateurs Rue de Genève 7 Case postale 6151 1002 Lausanne
IVSK COAI	IV-Stellen-Konferenz Conference des offices AI

COAI	Conferenza degli Uffici AI Landenbergstr. 35 6005 Luzern
kf	Konsumentenforum kf Grossmannstr. 29 8049 Zürich
KKA	Konferenz der kantonalen Ausgleichskassen p.a. Ausgleichskasse des Kt. Bern Chutzenstr. 10 3007 Bern
kv schweiz sec suisse sic svizzera	Kaufmännischer Verband Schweiz Société suisse des employés de commerce Società svizzera degli impiegati del commercio Zentralsekretariat Hans-Huber-Str. 4 8027 Zürich
privatim	Die Schweizerischen Datenschutzbeauftragten Les commissaires suisses à la protection des données c/o Datenschutzbeauftragter des Kantons Zürich Kaspar Escher-Haus 8090 Zürich
santésuisse	Die Schweizer Krankenversicherer Les assureurs-maladie suisses Römerstr. 20 Postfach 4502 Solothurn
SBV USP USC	Schweiz. Bauernverband Union Suisse des Paysans Unione Svizzera dei Contadini Laurstr. 10 5201 Brugg
SDV ASMD ASMD	Schweizer Direktmarketing Verband Association Suisse de Marketing Direct Postfach 616 8501 Frauenfeld
SGB USS USS	Schweizerischer Gewerkschaftsbund Union syndicale suisse Unione sindacale svizzera Monbijoustr. 61 3007 Bern

SGV USAM USAM	Schweizerischer Gewerbeverband Union suisse des arts et métiers Unione svizzera delle arti e mestieri Schwarztorstr. 26 3001 Bern
Stiftung Konsumentenschutz	Stiftung für Konsumentenschutz Monbijoustr. 3000 Bern 23
SVV ASA ASA	Schweizerischer Versicherungsverband Association Suisse d'Assurances Associatione Svizzera d'Assicurazioni C.F.Meyer-Strasse 14 Postfach 4288 8022 Zürich
swico	Schweiz. Wirtschaftsverband der Informations-, Kommunikations- und Organisationstechnik Association économique suisse de la bureautique, de l'informatique, de la télématique Technoparkstrasse 1 CH-8005 Zürich / Schweiz
swissbanking	Schweizerische Bankiervereinigung Association suisse des banquiers Associazione Svizzera dei Banchieri Aeschenplatz 7 Postfach 4182 4002 Basel
VVAK	Schweizerische Vereinigung der Verbandsausgleichskassen p.a. Ausgleichskasse EXFOUR Malzgasse 16 4010 Basel

2. Behörden, Organisationen und Private, welche zusätzlich zu den Anhörungsadressaten eine Stellungnahme abgegeben haben (10)

2.1 Bundesbehörden

EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter Préposé fédéral à la protection des données et à la transparence

EKK	Eidg. Kommission für Konsumentenfragen Commission fédérale de la consommation Effingerstr. 27 3003 Bern
SECO (SAS)	Staatssekretariat für Wirtschaft Schweizerische Akkreditierungsstelle Lindenweg 50 3003 Bern-Wabern

2.2 Organisationen

Groupe Mutuel	Groupe Mutuel Rue du Nord 5 1920 Martigny
RVK	RVK – Verband der kleinen und mittleren Krankenversicherer Haldenstr. 25 6006 Luzern
SGS	Societé Générale de Surveillance SA Technoparkstr. 1 8005 Zürich
VSK UBC UBC	Verband Schweizerischer Kantonalbanken Union des Banques Cantonales Suisses Unione delle Banche Cantonali Svizzere Wallstrasse 8 Postfach 4002 Basel
VSMS ASMS ASMS	Verband Schweizer Markt- und Sozialforscher Association suisse des spécialistes en recherches de marché et sociales Associazione svizzera dei specialisti in ricerche di mercato e sociali Gewerbestr. 5 6330 Cham

2.3 Private

Belser	Belser Datenschutz GmbH Schwarztorstr. 87 3007 Bern
Bär&Karrer	Bär & Karrer Rechtsanwälte Brandschenkestr. 90 8027 Zürich