Vernehmlassung zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz
Tabelle Stellungnahme

Entwurf VDSG	**Bemerkungen/Anregungen**
Art. 3 Protokollierung [1] Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht, protokollieren der private Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten. [2] Bundesorgane und deren Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten. (…)	Bemerkung: Die umfassende Protokollierungspflicht für Bundesorgane geht zu weit und ist nicht angemessen. Es können in diesem Punkt für Bundesorgane die gleichen Anforderungen wie für private Verantwortliche angewendet werden. Änderungsvorschlag: [1] Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der automatisierten Bearbeitung von Personendaten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht, protokollieren der ~~private~~ Verantwortliche und dessen Auftragsbearbeiter zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten. ~~[2] Bundesorgane und deren Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest folgende Vorgänge: das Speichern, Verändern, Lesen, Bekanntgeben, Löschen oder Vernichten.~~
Art. 4 Bearbeitungsreglement von privaten Personen [1] Der Verantwortliche und dessen Auftragsbearbeiter müssen ein Reglement für automatisierte Bearbeitungen erstellen, wenn sie: a. umfangreich besonders schützenswerte Personendaten bearbeiten; oder b. ein Profiling mit hohem Risiko durchführen. (…) [3] Die private Person muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.	Bemerkung zu Abs. 1: Zunächst ist die Eingrenzung der Pflicht zur Erstellung eines Reglements auf die Fälle nach Abs. 1 Bst. a und b zu eng. Die Revision des DSG ist gekennzeichnet durch einen risikobasierten Ansatz. In zahlreichen Bestimmungen werden Rechtswirkungen an das Vorliegen eines «hohen Risikos für die Persönlichkeit oder die Grundrechte der betroffenen Person» angeknüpft. Es ist nicht ersichtlich, weshalb von diesem Massstab – der u.a. für die Erstellung einer Datenschutz-Folgenabschätzung gilt (vgl. Art. 22 Abs. 1 nDSG) – vorliegend abgewichen wird. Ein hohes Risiko kann etwa bei der Bearbeitung von umfangreichen gewöhnlichen Personendaten bestehen. Immerhin können die Buchstaben a und b als nicht abschliessende Beispiele, für Fälle in denen stets ein hohes Risiko vorliegt, beibehalten werden.

	Änderungsvorschlag zu Abs. 1: [1] Der Verantwortliche und dessen Auftragsbearbeiter müssen ein Reglement für automatisierte Bearbeitungen erstellen, wenn **die Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Ein hohes Risiko liegt namentlich vor, wenn:** a. umfangreich besonders schützenswerte Personendaten bearbeiten; oder b. ein Profiling mit hohem Risiko durchführen. Bemerkung zu Abs. 3: Ferner ist unklar was mit dem Zusatz in Absatz 3, wonach das Reglement in einer für die Datenschutzberaterin oder den Datenschutzberater «verständlichen Form» zur Verfügung gestellt werden muss, gemeint ist. Unverständlich darf das Bearbeitungsreglement nie sein. Das versteht sich von selbst. Dass das Reglement allenfalls für Laien unverständlich sein kann, ist unbeachtlich, handelt es sich bei der Datenschutzberaterin oder dem Datenschutzberater doch um eine qualifizierte Fachperson (vgl. Art. 10 Abs. 3 Bst. c nDSG sowie Art. 28 Abs. 1 Bst. a E-VDSG). Schliesslich sollte zumindest in den Erläuterungen klargestellt werden, dass die Bestellung einer Datenschutzberaterin oder eines Datenschutzberaters gemäss Art. 10 nDSG freiwillig erfolgt. Änderungsvorschlag zu Abs. 3: [3] Die private Person muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater ~~in einer für diese oder diesen verständlichen Form~~ zur Verfügung stellen.
Art. 5 Bearbeitungsreglement von Bundesorganen (…) [3] Das verantwortliche Bundesorgan muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form sowie dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auf Anfrage zur	Bemerkung: Es kann auf die Bemerkung zu Art. 4 E-VDSG verwiesen werden. Änderungsvorschlag: [3] Das verantwortliche Bundesorgan muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater ~~in einer für diese oder diesen verständlichen Form~~ sowie dem Eidgenössischen

Verfügung stellen.	Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auf Anfrage zur Verfügung stellen
Art. 7 Information an die Datenschutzberaterin oder den Datenschutzberater des Bundesorgans Das Bundesorgan informiert die Datenschutzberaterin oder den -berater umgehend über den Abschluss eines Vertrags mit einem Auftragsbearbeiter oder die Genehmigung zur Übertragung der Datenbearbeitung an einen Dritten. Überdies informiert es diese oder diesen, wenn Probleme bei der Einhaltung der gesetzlichen oder vertraglichen Datenschutzvorschriften entstehen.	Bemerkung: Art. 7 ist überflüssig und irreführend. Gemäss Art. 10 Abs. 2 Bst. b nDSG wirkt der Datenschutzberater ohnehin bei der Anwendung der Datenschutzvorschriften mit. Dieser Anforderung trägt Art. 7 zu wenig Rechnung, indem der Berater erst *nach* Abschluss eines Auftragsbearbeitungsvertrages informiert wird. Im Übrigen bringt die Bestimmung keinen Mehrwert und kann demnach ersatzlos gestrichen werden. Änderungsvorschlag: ~~Das Bundesorgan informiert die Datenschutzberaterin oder den -berater umgehend über den Abschluss eines Vertrags mit einem Auftragsbearbeiter oder die Genehmigung zur Übertragung der Datenbearbeitung an einen Dritten. Überdies informiert es diese oder diesen, wenn Probleme bei der Einhaltung der gesetzlichen oder vertraglichen Datenschutzvorschriften.~~
Art. 12 Verhaltenskodizes und Zertifizierungen (…) [3] Der Verhaltenskodex oder die Zertifizierung muss mit einer verbindlichen und durchsetzbaren Verpflichtung des Verantwortlichen oder des Auftragsbearbeiters im Drittstaat verbunden werden, die darin enthaltenen Massnahmen anzuwenden.	Bemerkung: Der Charakter der «durchsetzbaren Verpflichtung» ist zu präzisieren. In gewissen Staaten werden rechtliche Verpflichtungen rein theoretisch zwar durchsetzbar sein, praktisch gesehen dürften die realistischen Durchsetzungsmöglichkeiten aber gering bleiben, sei dies aufgrund von rechtlichen Hürden, überlasteter Verwaltung und Justiz, Korruption oder dergleichen. Wichtig ist, dass die Durchsetzbarkeit der Verpflichtung ohne unverhältnismässigen Aufwand möglich ist. Im Übrigen sollte aus den Erläuterungen klar hervorgehen, dass Verhaltenskodizes nur von Verbänden und nicht von einzelnen Verantwortlichen stammen können (vgl. Botschaft nDSG, 7035). Änderungsvorschlag: [3] Der Verhaltenskodex oder die Zertifizierung muss mit einer verbindlichen und **mit verhältnismässigen Aufwand** durchsetzbaren Verpflichtung des Verantwortlichen oder des Auftragsbearbeiters im Drittstaat verbunden werden, die darin enthaltenen Massnahmen anzuwenden.

Art. 13 Modalitäten der Informationspflicht [1] Der Verantwortliche und der Auftragsbearbeiter teilen die Information über die Beschaffung von Personendaten in präziser, verständlicher und leicht zugänglicher Form mit. [2] Teilt er die Informationen in Kombination mit Piktogrammen mit, die elektronisch dargestellt werden, so müssen diese maschinenlesbar sein.	Bemerkung: Zu begrüssen ist, dass darauf verzichtet wird die Information durch einen sogenannten Medienbruch allgemein zu legitimieren. Ein Medienbruch liegt beispielsweise dann vor, wenn in einem abgedruckten Vertrag auf einen QR-Code oder bei einem Telefonat auf einen URL-Link verwiesen wird, worüber die betroffene Person an die zu erteilenden Informationen gelangen kann. Ob der Informationspflicht durch derartige Informationsmethoden genüge getan ist, muss anhand von Art. 19 Abs. 1 nDSG beurteilt werden, wonach die Information «angemessen» zu sein hat. Es gelten dabei der Verhältnismässigkeitsgrundsatz und der risikobasierte Ansatz. Es sind die aus der Datenbearbeitung resultierenden Risiken für die betroffene Person und der Aufwand des Verantwortlichen für die Informationserbringung gegeneinander abzuwägen. Bei einer Bearbeitung von besonders schützenswerten Personendaten wird die Information über einen Medienbruch regelmässig unangemessen sein und somit den gesetzlichen Anforderungen nicht genügen. Eine allgemeine und pauschale Legitimierung des Medienbruchs – wie teilweise gefordert – ist abzulehnen.
Art. 20 Modalitäten [1] Das Auskunftsbegehren wird schriftlich gestellt. Ist der Verantwortliche einverstanden, so kann das Begehren auch mündlich gestellt werden. (…)	Bemerkung: Art. 25 nDSG schreibt die Schriftlichkeit eines Auskunftsbegehrens nicht mehr vor. Der erste Satz von Art. 20 Abs. 1 E-VDSG verlangt eine solche jedoch in absoluter Form. Diese wird zwar durch Satz 2 relativiert. Die Bestimmung ist dadurch aber widersprüchlich, und der erste Satz verletzt in dieser Form Art. 25 nDSG. Ein Auskunftsbegehren soll generell in schriftlicher und in mündlicher Form möglich sein. Dies hat gleichzeitig zur Folge, dass das Gesuch auch denjenigen Personen offensteht, für welche die Schriftlichkeit eine schwer oder nicht überwindbare Hürde darstellen würde. Änderungsvorschlag: [1] Das Auskunftsbegehren ~~wird~~ **kann** schriftlich **oder mündlich** gestellt **werden**. ~~Ist der Verantwortliche einverstanden, so kann das Begehren auch mündlich gestellt werden~~
Art. 21 Zuständigkeit [1] Sind für die Bearbeitung von Personendaten mehrere verantwortlich, so	Bemerkung: Der zweite Satz von Abs. 1 bewirkt für private Verantwortliche einen

kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen. Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter. (…)	unverhältnismässigen Aufwand. Für Bundesorgane ergibt sich dieser Grundsatz hingegen ohnehin aus dem Verwaltungsrecht. Insofern kann der zweite Satz ersatzlos gestrichen werden. Änderungsvorschlag: [1] Sind für die Bearbeitung von Personendaten mehrere verantwortlich, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen. ~~Ist ein Verantwortlicher für die Behandlung des Begehrens nicht zuständig, so leitet er es an den zuständigen Verantwortlichen weiter.~~
Art. 22 Frist [1] Die Auskunft wird innert 30 Tagen seit dem Eingang des Begehrens erteilt. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen. [2] Kann die Auskunft nicht innert 30 Tagen erteilt werden, so muss der Verantwortliche die betroffene Person darüber benachrichtigen und ihr die Frist mitteilen, in der die Auskunft erfolgen wird.	Bemerkung: Damit eindeutig klar ist, dass die Auskunft *in der Regel* innert 30 Tagen erteilt wird, wie es Art. 25 Abs. 7 nDSG verlangt, sollte dies auch aus der Verordnungsbestimmung explizit hervorgehen. Änderungsvorschlag: [1] Die Auskunft wird **in der Regel** innert 30 Tagen seit dem Eingang des Begehrens erteilt. Wenn der Verantwortliche die Auskunft verweigert, einschränkt oder aufschiebt, muss er dies innert derselben Frist mitteilen. Bemerkung: Aus dem Wortlaut von Absatz 2 muss klar hervorgehen, dass die Überschreitung der 30-tägigen Frist die *Ausnahme* bleibt. Ausserdem ist sicherzustellen, dass die verlängerte Frist *angemessen* bleibt und nicht nach Belieben des Verantwortlichen ausfallen kann. Änderungsvorschlag: [2] Kann die Auskunft **ausnahmsweise** nicht innert 30 Tagen erteilt werden, so muss der Verantwortliche die betroffene Person darüber benachrichtigen und ihr ~~die~~ **eine angemessene** Frist mitteilen, in der die Auskunft erfolgen wird.
Art. 23 Ausnahmen von der Kostenlosigkeit (…) [2] Die Beteiligung beträgt maximal 300 Franken.	Bemerkung: Es ist zu begrüssen, dass der Kostenbeteiligung in Absatz 2 klare und für die betroffenen Personen verhältnismässige Grenzen gesetzt werden. Weil Auskunftsgesuche in Ausnahmefällen aber einen beträchtlichen Aufwand für

(…)	Verantwortliche generieren können, ist fraglich, ob eine Obergrenze von maximal CHF 500 zu bevorzugen wäre. Abzulehnen weil unzumutbar sind indessen sicherlich Kostenbeteiligungen im vierstelligen Bereich. Änderungsvorschlag: [2] Die Beteiligung beträgt maximal **500** Franken.
Art. 26 Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt. a. Es werden umfangreich besonders schützenswerte Personendaten bearbeitet. b. Es wird ein Profiling mit hohem Risiko durchgeführt.	Bemerkung: Die Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten für die Konstellationen nach Bst. a und b zu weit. Es ist nicht ersichtlich, weshalb vom Massstab zur Erstellung einer Datenschutz-Folgenabschätzung, wie in Art. 22 Abs. 1 nDSG vorgesehen, abgewichen wird. Dieser risikobasierte Massstab (*hohes Risiko* für die Persönlichkeit oder die Grundrechte der betroffenen Person) durchzieht das nDSG und ist auch hier zu übernehmen. Immerhin können die Buchstaben a und b als nicht abschliessende Beispiele für, wann ein hohes Risiko vorliegt, beibehalten werden. Änderungsvorschlag: Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, **sofern ihre Bearbeitungstätigkeiten kein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen. Ein hohes Risiko liegt namentlich vor, wenn:** ~~ausser eine der folgenden Voraussetzungen ist erfüllt.~~ a. Es werden umfangreich besonders schützenswerte Personendaten bearbeitet. b. Es wird ein Profiling mit hohem Risiko durchgeführt.
Verordnung über das Strafregister vom 29. September 2006 (VOSTRA-Verordnung; SR 331) Art. 18 Sorgfaltspflichten und Datenbearbeitungsgrundsätze (…)	Bemerkung: Mit Inkrafttreten des Strafregistergesetzes, voraussichtlich 2023, wird den kantonalen Polizeistellen Zugriff auf das Strafregister gewährt, u.a. für die Erkennung oder Verhütung von Straftaten (Art. 38 i.V.m. Art. 46). Für die Polizei werden u.a. Grundurteile ersichtlich, die ein Tätigkeitsverbot oder ein

[5] Die Strafregisterdaten nach Artikel 366 Absätze 2 bis 4 StGB dürfen nicht isoliert in einer neuen Datenbank gespeichert oder aufbewahrt werden, es sei denn, dies sei zur Begründung eines getroffenen Entscheides, einer erlassenen Verfügung oder eines eingeleiteten Verfahrensschritts notwendig. (…)	Kontakt- und Rayonverbot nach Art. 67 ff. StGB enthalten. Die Kenntnis eines solchen Verbots ist primär zur Verbotsdurchsetzung von Bedeutung, konkret zur Gewährleistung, dass der Verbotszweck (Verhinderung einer weiteren, schweren Straftat) tatsächlich erreicht wird. Das zentrale Informationssystem der Polizei enthält u.a. Hinweise über geltende Wegweisungen und Rückkehrverbote nach ZGB und nach kantonalem Recht. Zur Gefahrenabwehr und Straftatenverhütung stehen die Daten insb. den intervenierenden Polizeiangehörigen vor Ort zur Verfügung. Dasselbe sollte auch für die Verbote nach Art. 67 ff. StGB möglich sein, dürfte von engen Wortlaut im Entwurf allerdings nicht gedeckt sein. Änderungsvorschlag: [5] Die Strafregisterdaten nach Artikel 366 Absätze 2 bis 4 StGB dürfen nicht isoliert in einer neuen Datenbank gespeichert oder aufbewahrt werden, es sei denn, dies sei zur Begründung **oder Durchsetzung** eines getroffenen Entscheides, einer erlassenen Verfügung oder eines eingeleiteten Verfahrensschritts notwendig.