Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

vom …

Der Schweizerische Bundesrat,

gestützt auf die Artikel 8 Absatz 3, 10 Absatz 4, 12 Absatz 5, 16 Absatz 3, 25 Absatz 6, 28 Absatz 3, 33, 59 Absätze 2 und 3 des Bundesgesetzes vom 25. September 2020[1] über den Datenschutz (DSG)

verordnet:

1. Kapitel: Allgemeine Bestimmungen

1. Abschnitt: Datensicherheit

Art. 1 Grundsätze

[1] Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien:

a. Zweck, Art, Umfang und Umstände der Datenbearbeitung;

b. die Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren potenziellen Auswirkungen für die betroffenen Personen;

c. der Stand der Technik;

d. Implementierungskosten.

[2] Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen.

Art. 2 Schutzziele

Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele erreichen:

1 SR **235.1**

a. Zugriffskontrolle: Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten beschränkt, die sie zur Erfüllung ihrer Aufgabe benötigen.

b. Zugangskontrolle: Der Zugang zu den Einrichtungen und Anlagen, in denen Personendaten bearbeitet werden, wird unbefugten Personen verwehrt.

c. Datenträgerkontrolle: Das Lesen, Kopieren, Verändern, Verschieben oder Entfernen von Datenträgern wird unbefugten Personen verunmöglicht.

d. Speicherkontrolle: Unbefugte Eingabe in den Datenspeicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten wird verhindert.

e. Benutzerkontrolle: Die Benutzung von automatisierten Datenbearbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen wird verhindert.

f. Transportkontrolle: Bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern wird verhindert, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

g. Eingabekontrolle: In automatisierten Systemen kann überprüft werden, welche Personendaten zu welcher Zeit und von welcher Person eingegeben oder verändert wurden.

h. Bekanntgabekontrolle: Es kann überprüft werden, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekannt gegeben wurden.

i. Wiederherstellung: Die Verfügbarkeit der Personendaten und der Zugang zu ihnen kann bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden.

j. Es wird gewährleistet, dass alle Funktionen des Systems zur Verfügung stehen (Verfügbarkeit), auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).

k. Erkennung: Verletzungen der Datensicherheit können rasch erkannt und Massnahmen zur Minderung oder Beseitigung der Folgen eingeleitet werden.

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.

3 Die Protokollierung gibt Aufschluss über die Art des Bearbeitungsvorgangs, die Identität der Person, die die Bearbeitung vorgenommen hat, die Identität der Empfängerin oder des Empfängers sowie den Zeitpunkt, an dem die Bearbeitung erfolgt ist.

4 Die Protokolle sind während zwei Jahren getrennt vom System, in welchem die Personendaten bearbeitet werden, aufzubewahren. Sie sind ausschliesslich den Organen oder Personen zugänglich, denen die Überwachung der Datenschutzvorschriften oder die Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegen, und dürfen nur für diesen Zweck verwendet werden.

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.

2 Das Reglement muss mindestens Angaben enthalten:

a. zum Bearbeitungszweck;

b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;

c. zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;

d. zur internen Organisation;

e. zur Herkunft der Personendaten und zur Art ihrer Beschaffung;

f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit;

g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe;

h. zu den Massnahmen, die zur Datenminimierung getroffen werden;

i. zu den Datenbearbeitungsverfahren, insbesondere den Verfahren bei der Speicherung, Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung, Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung;

j. zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung.

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

1 Das verantwortliche Bundesorgan und dessen Auftragsbearbeiter erstellen ein Bearbeitungsreglement für automatisierte Bearbeitungen, wenn sie:

a. besonders schützenswerte Personendaten bearbeiten;

b. ein Profiling durchführen;

c. Datenbearbeitungen im Sinne von Artikel 34 Absatz 2 Buchstabe c DSG ausführen;

d. Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen werden Personendaten zugänglich machen;

e. Datenbestände miteinander verknüpfen; oder

f. mit anderen Bundesorganen zusammen ein Informationssystem betreiben oder Datenbestände bewirtschaften.

2 Das Reglement muss mindestens die Angaben nach Artikel 4 Absatz 2 enthalten.

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 Verfügung stellen.

2. Abschnitt: Bearbeitung durch Auftragsbearbeiter

Art. 6 Modalitäten

1 Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz verantwortlich. Er muss sicherstellen, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.

2 Untersteht der Auftragsbearbeiter dem DSG nicht, so muss sich der Verantwortliche vergewissern, dass andere gesetzliche Bestimmungen einen gleichwertigen Datenschutz gewährleisten. Andernfalls muss er diesen auf vertraglichem Wege sicherstellen.

3 Handelt es sich beim Verantwortlichen um ein Bundesorgan, so darf der Auftragsbearbeiter die Datenbearbeitung einem Dritten übertragen, wenn das Bundesorgan dies schriftlich genehmigt hat.

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.

3. Abschnitt: Bekanntgabe von Personendaten ins Ausland

Art. 8 Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internationalen Organs

[1] Werden Personendaten ins Ausland bekanntgegeben, so müssen bei der Beurteilung, ob ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, namentlich die folgenden Kriterien berücksichtigt werden:

a. die internationalen Verpflichtungen des Staates oder internationalen Organs im Bereich des Datenschutzes;

b. die Achtung der Menschenrechte;

c. die geltende Gesetzgebung zum Datenschutz sowie deren Umsetzung und die einschlägige Rechtsprechung;

d. die wirksame Gewährleistung der Rechte der betroffenen Personen und des Rechtsschutzes;

e. das wirksame Funktionieren von einer oder mehreren unabhängigen Behörden, die im betreffenden Staat mit dem Datenschutz beauftragt sind oder denen ein internationales Organ untersteht und die über ausreichende Befugnisse und Kompetenzen verfügen.

[2] Bei der Beurteilung können die Einschätzungen von internationalen Organen oder ausländischen Behörden, die für den Datenschutz zuständig sind, berücksichtigt werden.

[3] Die Angemessenheit des Datenschutzes des betreffenden Staates, des Gebiets, der spezifischen Sektoren in einem Staat oder des internationalen Organs wird periodisch neu beurteilt.

[4] Ergibt sich aus einer Beurteilung nach Absatz 3 oder aus verfügbaren Informationen, dass ein Staat, ein Gebiet, einer oder mehrere spezifische Sektoren in einem Staat oder ein internationales Organ kein angemessener Datenschutz mehr gewährleistet, so wird der Entscheid gemäss Artikel 16 Absatz 1 DSG geändert, sistiert oder aufgehoben. Dieser neue Entscheid hat keine Auswirkungen auf bereits erfolgte Datenbekanntgaben.

[5] Die Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organe mit einem angemessenen Datenschutz sind in Anhang 1 aufgeführt.

[6] Der EDÖB wird vor jedem Entscheid über die Angemessenheit des Datenschutzes konsultiert.

Art. 9 Datenschutzklauseln und spezifische Garantien

[1] Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen mindestens die folgenden Punkte regeln:

a. die Anwendung der Grundsätze der Rechtmässigkeit, von Treu und Glauben, der Verhältnismässigkeit, der Zweckbindung und der Richtigkeit;

b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen Personen;

c. die Art und der Zweck der Bekanntgabe von Personendaten;

d. die Namen der Staaten, in die Personendaten bekanntgegeben werden;

e. die Namen der internationalen Organe, denen Personendaten bekanntgegeben werden;

f. die Anforderungen an die Aufbewahrung, die Löschung und die Vernichtung von Personendaten;

g. die zur Bearbeitung der Daten berechtigten Empfängerinnen und Empfänger;

h. die Massnahmen zur Gewährleistung der Datensicherheit;

i. die Anforderungen an eine Bekanntgabe von Personendaten in einen anderen ausländischen Staat oder an ein anderes internationales Organ;

j. die Pflicht der Empfängerin oder des Empfängers, die betroffenen Personen über die Bearbeitung zu informieren;

k. die Rechte der betroffenen Person, namentlich:
   1. das Auskunftsrecht,
   2. das Widerspruchsrecht,
   3. das Recht auf Berichtigung, Löschung oder Vernichtung ihrer Daten,
   4. das Recht, eine unabhängige Behörde um Rechtsschutz zu ersuchen.

[2] Der Verantwortliche muss angemessene Massnahmen treffen, um sicherzustellen, dass die Empfängerin oder der Empfänger die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien einhält.

[3] Wurde der EDÖB über die Datenschutzklauseln in einem Vertrag oder die spezifischen Garantien informiert, so gilt die Informationspflicht für alle weiteren Bekanntgaben als erfüllt, die:

a. unter denselben Datenschutzklauseln oder Garantien erfolgen, soweit die Kategorien der Empfängerinnen und Empfänger, der Zweck der Bearbeitung und die Datenkategorien im Wesentlichen unverändert bleiben; oder

b. innerhalb derselben juristischen Person oder Gesellschaft oder zwischen Unternehmen, die zum selben Konzern gehören, stattfinden, soweit die Datenschutzklauseln oder Garantien weiterhin einen geeigneten Datenschutz gewährleisten.

Art. 10 Standarddatenschutzklauseln

[1] Gibt der Verantwortliche Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so trifft er angemessene

Massnahmen, um sicherzustellen, dass die Empfängerin oder der Empfänger diese beachtet.

[2] Der EDÖB veröffentlicht eine Liste von Standarddatenschutzklauseln, die er genehmigt, ausgestellt oder anerkannt hat.

Art. 11 Verbindliche unternehmensinterne Datenschutzvorschriften

[1] Verbindliche unternehmensinterne Datenschutzvorschriften nach Artikel 16 Absatz 2 Buchstabe e DSG gelten für alle Unternehmen, die zum selben Konzern gehören.

[2] Sie umfassen mindestens die in Artikel 9 Absatz 1 genannten Punkte sowie die folgenden Angaben:

a. die Organisation und die Kontaktdaten des Konzerns und seiner Unternehmen;

b. die innerhalb des Konzerns getroffenen Massnahmen zur Gewährleistung der Einhaltung der verbindlichen unternehmensinternen Datenschutzvorschriften.

Art. 12 Verhaltenskodizes und Zertifizierungen

[1] Personendaten dürfen ins Ausland bekannt gegeben werden, wenn durch einen Verhaltenskodex oder eine Zertifizierung ein geeigneter Datenschutz gewährleistet wird.

[2] Der Verhaltenskodex enthält mindestens die Angaben nach Artikel 9 Absatz 1 und muss vorgängig vom EDÖB genehmigt werden.

[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.

2. Kapitel: Pflichten des Verantwortlichen und des Auftragsbearbeiters

Art. 13 Modalitäten der Informationspflichten

[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.

Art. 14 Informationspflicht der Bundesorgane bei der systematischen Beschaffung von Personendaten

Ist die betroffene Person nicht zur Auskunft verpflichtet, so weist das verantwortliche Bundesorgan sie bei einer systematischen Beschaffung von Personendaten, insbesondere mittels Fragebogen, auf die Freiwilligkeit der Auskunftserteilung hin.

Art. 15 Information bei der Bekanntgabe von Personendaten

Der Verantwortliche und der Auftragsbearbeiter informieren die Empfängerin oder den Empfänger über die Aktualität, Zuverlässigkeit und Vollständigkeit der von ihnen bekannt gegebenen Personendaten, soweit sich diese Informationen nicht aus den Daten selbst oder aus den Umständen ergeben.

Art. 16 Information über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten

Der Verantwortliche informiert die Empfängerinnen und Empfänger, denen er Personendaten bekanntgegeben hat, unverzüglich über die Berichtigung, Löschung oder Vernichtung sowie die Einschränkung der Bearbeitung von Personendaten, ausser die Benachrichtigung ist unmöglich oder mit einem unverhältnismässigen Aufwand verbunden.

Art. 17 Überprüfung einer automatisierten Einzelentscheidung

Verlangt eine von einer automatisierten Einzelentscheidung betroffene Person, dass sie ihren Standpunkt darlegen kann oder dass eine natürliche Person die Entscheidung überprüft, so darf sie deswegen nicht benachteiligt werden.

Art. 18 Form und Aufbewahrung der Datenschutz-Folgenabschätzung

Der Verantwortliche muss die Datenschutz-Folgenabschätzung schriftlich festhalten. Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden.

Art. 19 Meldung von Verletzungen der Datensicherheit

[1] Der Verantwortliche meldet dem EDÖB bei einer Verletzung der Datensicherheit:

a. die Art der Verletzung;
b. soweit möglich den Zeitpunkt und die Dauer;
c. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personendaten;
d. soweit möglich die Kategorien und ungefähre Anzahl der betroffenen Personen;
e. die Folgen, einschliesslich der allfälligen Risiken, für die betroffenen Personen;

f. welche Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben oder die Folgen zu mildern;

g. den Namen und die Kontaktdaten einer Ansprechperson.

[2] Ist es dem Verantwortlichen bei Entdeckung der Verletzung der Datensicherheit nicht möglich, dem EDÖB alle Informationen gemäss Absatz 1 zur gleichen Zeit bereitzustellen, so kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

[3] Der Verantwortliche teilt den betroffenen Personen in einfacher und verständlicher Sprache mindestens die Informationen nach Absatz 1 Buchstaben a, e, f und g mit.

[4] Handelt es sich beim Verantwortlichen um ein Bundesorgan, so erfolgt die Meldung an den EDÖB über die Datenschutzberaterin oder den Datenschutzberater.

[5] Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens drei Jahre aufzubewahren.

3. Kapitel: Rechte der betroffenen Person

1. Abschnitt: Auskunftsrecht

Art. 20 Modalitäten

[1] Das Auskunftsbegehren wird schriftlich gestellt. Ist der Verantwortliche einverstanden, so kann das Begehren auch mündlich gestellt werden.

[2] Die Auskunft wird in der Regel schriftlich erteilt. Im Einvernehmen mit dem Verantwortlichen oder auf dessen Vorschlag hin kann die betroffene Person ihre Daten auch an Ort und Stelle einsehen. Die Auskunft kann auch mündlich erteilt werden, wenn die betroffene Person eingewilligt hat.

[3] Die Auskunft muss für die betroffene Person verständlich sein.

[4] Der Verantwortliche muss die angemessenen Massnahmen treffen, um die Identifizierung der betroffenen Person sicherzustellen und die Personendaten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen. Die betroffene Person muss bei ihrer Identifizierung mitwirken.

[5] Der Verantwortliche hat die Gründe für eine Verweigerung, Einschränkung oder den Aufschub der Auskunft zu dokumentieren. Die Dokumentation ist mindestens drei Jahre lang aufzubewahren.

Art. 21 Zuständigkeit

[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.

2 Betrifft das Begehren Daten, die von einem Auftragsbearbeiter bearbeitet werden, so leitet der Verantwortliche das Begehren an den Auftragsbearbeiter weiter, sofern er nicht in der Lage ist, selbst Auskunft zu erteilen.

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.

Art. 23 Ausnahmen von der Kostenlosigkeit

1 Eine angemessene Beteiligung an den Kosten kann verlangt werden, wenn die Auskunftserteilung mit einem unverhältnismässigen Aufwand verbunden ist.

2 Die Beteiligung beträgt maximal 300 Franken.

3 Die betroffene Person ist über die Höhe der Beteiligung vor der Auskunftserteilung in Kenntnis zu setzen und kann ihr Gesuch innert zehn Tagen zurückziehen.

2. Abschnitt: Recht auf Datenherausgabe oder -übertragung

Art. 24

Die Artikel 20 Absätze 1, 4 und 5, sowie 21, 22 und 23 sind auf das Recht auf Datenherausgabe und -übertragung sowie deren Einschränkungen sinngemäss anwendbar.

4. Kapitel: Besondere Bestimmungen zur Datenbearbeitung durch private Personen

Art. 25 Datenschutzberaterin oder Datenschutzberater

1 Die Datenschutzberaterin oder der Datenschutzberater eines privaten Verantwortlichen muss folgende Aufgaben wahrnehmen:

a. Sie oder er prüft die Bearbeitung von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass Datenschutzvorschriften verletzt wurden.

b. Sie oder er wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und überprüft diese, jedenfalls dann, wenn der private Verantwortliche von der Konsultation des EDÖB im Sinne von Art. 23 Abs. 4 DSG absehen will.

2 Der private Verantwortliche muss der Datenschutzberaterin oder dem Datenschutzberater:

a. die notwendigen Ressourcen zur Verfügung stellen;

b. Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten gewähren, die sie oder er zur Erfüllung ihrer oder seiner Aufgaben benötigt.

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.

5. Kapitel: Besondere Bestimmungen zur Datenbearbeitung durch Bundesorgane

1. Abschnitt: Datenschutzberaterin oder -berater

Art. 27 Ernennung

Jedes Bundesorgan ernennt eine Datenschutzberaterin oder einen Datenschutzberater. Mehrere Bundesorgane können gemeinsam eine Datenschutzberaterin oder einen Datenschutzberater ernennen.

Art. 28 Anforderungen und Aufgaben

1 Die Datenschutzberaterin oder der Datenschutzberater muss die folgenden Anforderungen erfüllen:

a. Sie oder er verfügt über die erforderlichen Fachkenntnisse.

b. Sie oder er übt ihre oder seine Funktion gegenüber dem Bundesorgan fachlich unabhängig und weisungsungebunden aus.

2 Sie oder er muss folgende Aufgaben wahrnehmen:

a. Sie oder er prüft die Bearbeitung von Personendaten sowie deren Voraussetzungen und empfiehlt Korrekturmassnahmen, wenn sie oder er feststellt, dass Datenschutzvorschriften verletzt wurden.

b. Sie oder er wirkt bei der Erstellung der Datenschutz-Folgenabschätzung mit und überprüft diese.

c. Sie oder er meldet dem EDÖB Verletzungen der Datensicherheit.

d. Sie oder er dient als Anlaufstelle für die betroffenen Personen.

f. Sie oder er schult und berät das Bundesorgan sowie dessen Mitarbeiterinnen und Mitarbeiter in Fragen des Datenschutzes.

Art. 29 Pflichten des Bundesorgans

[1] Das Bundesorgan gewährt der Datenschutzberaterin oder dem Datenschutzberater Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten, die sie oder er zur Erfüllung ihrer oder seiner Aufgaben benötigt.

[2] Es veröffentlicht die Kontaktdaten der Datenschutzberaterin oder des Datenschutzberaters im Internet und teilt diese dem EDÖB mit.

Art. 30 Anlaufstelle des EDÖB

Die Datenschutzberaterin oder der Datenschutzberater dient dem EDÖB als Anlaufstelle für Fragen im Zusammenhang mit der Bearbeitung von Personendaten durch das betreffende Bundesorgan.

2. Abschnitt: Projekte von Bundesorganen zur automatisierten Bearbeitung von Personendaten

Art. 31 Information an die Datenschutzberaterin oder den Datenschutzberater

Das verantwortliche Bundesorgan informiert die Datenschutzberaterin oder den Datenschutzberater rechtzeitig bei der Planung eines Projektes zur automatisierten Bearbeitung von Personendaten sowie bei Anpassungen nach Abschluss des Projekts, damit die Erfordernisse des Datenschutzes sogleich berücksichtigt werden.

Art. 32 Meldung an den EDÖB

[1] Das verantwortliche Bundesorgan meldet dem EDÖB die geplanten automatisierten Bearbeitungstätigkeiten im Zeitpunkt der Projektfreigabe oder des Entscheids zur Projektentwicklung. Der EDÖB nimmt diese Meldung in das Register der Bearbeitungstätigkeiten auf.

[2] Die Meldung muss die Angaben nach Artikel 12 Absatz 2 Buchstaben a-d DSG sowie das voraussichtliche Datum des Beginns der Bearbeitungstätigkeiten enthalten.

[3] Das verantwortliche Bundesorgan aktualisiert die Meldung beim Übergang in den produktiven Betrieb oder bei der Projekteinstellung.

3. Abschnitt: Pilotversuche

Art. 33 Unentbehrlichkeit der Testphase

Eine Testphase als Pilotversuch ist unentbehrlich, wenn eine der folgenden Bedingungen erfüllt ist:

a. Die Erfüllung einer Aufgabe erfordert technische Neuerungen, deren Auswirkungen zunächst evaluiert werden müssen.

b. Die Erfüllung einer Aufgabe erfordert bedeutende organisatorische oder technische Massnahmen, deren Wirksamkeit zunächst geprüft werden muss, insbesondere bei der Zusammenarbeit zwischen Organen des Bundes und der Kantone.

c. Die Erfüllung der Aufgaben erfordert, dass die Personendaten mittels eines Abrufverfahrens zugänglich gemacht werden.

Art. 34 Bewilligung

1 Vor der Konsultation der interessierten Verwaltungseinheiten legt das für den Pilotversuch zuständige Bundesorgan zu Handen des EDÖB dar, wie die Einhaltung der Anforderungen nach Artikel 35 DSG gewährleistet werden soll, und lädt ihn zur Stellungnahme ein.

2 Der EDÖB nimmt zur Frage Stellung, ob die Bewilligungsvoraussetzungen nach Artikel 35 DSG erfüllt sind. Das zuständige Bundesorgan stellt ihm alle dazu notwendigen Unterlagen zur Verfügung, insbesondere:

a. eine allgemeine Beschreibung des Pilotversuchs;

b. einen Bericht, der nachweist, dass die Erfüllung der gesetzlich vorgesehenen Aufgaben die Bearbeitung im Sinne von Artikel 34 Absatz 2 DSG erfordert und dass eine Testphase vor dem Inkrafttreten des Gesetzes im formellen Sinn unentbehrlich ist (Artikel 35 Absatz 1 Buchstabe c DSG);

c. eine Beschreibung der internen Organisation sowie der Datenbearbeitungs- und Kontrollverfahren;

d. eine Beschreibung der Sicherheits- und Datenschutzmassnahmen;

e. den Entwurf einer Verordnung, welche die Einzelheiten der Bearbeitung regelt, oder das Konzept einer Verordnung;

f. die Informationen betreffend die Planung der verschiedenen Phasen des Pilotversuches.

3 Der EDÖB kann weitere Dokumente anfordern und zusätzliche Abklärungen vornehmen.

4 Das zuständige Bundesorgan informiert den EDÖB über jede wichtige Änderung, welche die Einhaltung der Anforderungen von Artikel 35 DSG betrifft. Der EDÖB nimmt, falls erforderlich, erneut Stellung.

5 Die Stellungnahme des EDÖB ist dem Antrag an den Bundesrat beizufügen.

6 Die Modalitäten der automatisierten Datenbearbeitung werden in einer Verordnung geregelt.

Art. 35 Evaluationsbericht

Das zuständige Bundesorgan legt dem EDÖB den Entwurf des Evaluationsberichts an den Bundesrat zur Stellungnahme vor. Die Stellungnahme des EDÖB ist dem Bundesrat zur Kenntnis zu bringen.

4. Abschnitt: Datenbearbeitung für nicht personenbezogene Zwecke

Art. 36

Werden Personendaten zu nicht personenbezogenen Zwecken, insbesondere Forschung, Planung und Statistik, und gleichzeitig zu einem anderen Zweck bearbeitet, so sind die Ausnahmen nach Artikel 39 Absatz 2 DSG nur für die Bearbeitung zu den nicht personenbezogenen Zwecken anwendbar.

6. Kapitel: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Art. 37 Sitz und ständiges Sekretariat

1 Der Sitz des EDÖB befindet sich in Bern.

2 Auf die Arbeitsverhältnisse der Angestellten des ständigen Sekretariats des EDÖB ist die Bundespersonalgesetzgebung anwendbar. Die Angestellten des ständigen Sekretariats des EDÖB sind im Rahmen des Vorsorgewerks Bund bei der Pensionskasse des Bundes PUBLICA gegen die wirtschaftlichen Folgen von Alter, Invalidität und Tod versichert.

Art. 38 Kommunikationsweg

1 Der EDÖB verkehrt mit dem Bundesrat über die Bundeskanzlerin oder den Bundeskanzler. Diese oder dieser leitet die Vorschläge, Stellungnahmen und Berichte unverändert an den Bundesrat weiter.

2 Er reicht Berichte zuhanden der Bundesversammlung über die Parlamentsdienste ein.

Art. 39 Mitteilung von Richtlinien und Entscheiden

1 Die Departemente und die Bundeskanzlei teilen dem EDÖB ihre Richtlinien im Bereich des Datenschutzes sowie ihre Entscheide in anonymisierter Form mit.

2 Die Bundesorgane legen dem EDÖB alle Rechtsetzungsentwürfe vor, welche die Bearbeitung von Personendaten, den Datenschutz sowie den Zugang zu amtlichen Dokumenten betreffen.

Art. 40 Bearbeitung von Personendaten

Der EDÖB bearbeitet Personendaten, einschliesslich besonders schützenswerter Personendaten, insbesondere zu folgenden Zwecken:

a. zur Ausübung seiner Aufsichtstätigkeiten;

b. zur Untersuchung von Verstössen gegen Datenschutzvorschriften;

c. zur Schulung und Beratung von Bundesorganen und privaten Personen;

d. zur Zusammenarbeit mit Bundesbehörden, kantonalen und ausländischen Behörden;

e. zur Durchführung von Schlichtungsverfahren und Evaluationen nach dem Bundesgesetz vom 17. Dezember 2004[2] über das Öffentlichkeitsprinzip der Verwaltung (BGÖ);

f. zur Beantwortung von Bürgeranfragen.

Art. 41 Selbstkontrolle

[1] Der EDÖB erstellt ein Bearbeitungsreglement für sämtliche automatisierten Bearbeitungen. Artikel 5 Absatz 1 findet keine Anwendung.

[2] Er sieht interne Prozesse vor, die gewährleisten, dass die Bearbeitungen entsprechend dem Bearbeitungsreglement vorgenommen werden. Er überprüft jährlich, ob das Bearbeitungsreglement eingehalten wird.

Art. 42 Zusammenarbeit mit dem Nationalen Zentrum für Cybersicherheit (NCSC)

[1] Der EDÖB kann die Angaben zur Meldung einer Verletzung der Datensicherheit zwecks Analyse des Vorfalls dem NCSC weiterleiten. Der EDÖB muss vorgängig das Einverständnis des meldepflichtigen Verantwortlichen einholen.

[2] Er lädt das NCSC zur Stellungnahme ein, bevor er gegenüber einem Bundesorgan eine Massnahme gemäss Artikel 51 Absatz 3 Buchstabe b DSG betreffend die Datensicherheit anordnet.

Art. 43 Register der Bearbeitungstätigkeiten der Bundesorgane

[1] Das Register der Bearbeitungstätigkeiten der Bundesorgane enthält die von den Bundesorganen und deren Auftragsbearbeiter gemachten Angaben nach Artikel 12 Absatz 2 und 3 DSG sowie Artikel 32 Absatz 2 dieser Verordnung.

[2] Es ist im Internet zu veröffentlichen. Nicht veröffentlicht werden die Registereinträge über geplante automatisierte Bearbeitungstätigkeiten nach Artikel 32.

2 SR **152.3**

Art. 44 Verhaltenskodizes

Wird dem EDÖB ein Verhaltenskodex vorgelegt, so teilt dieser in seiner Stellungnahme mit, ob der Verhaltenskodex die Voraussetzungen nach Artikel 22 Absatz 5 Buchstabe a und b DSG erfüllt.

Art. 45 Gebühren

[1] Die vom EDÖB in Rechnung gestellten Gebühren bemessen sich nach dem Zeitaufwand.

[2] Es gilt ein Stundenansatz von 150 bis 350 Franken. Dieser richtet sich nach der Komplexität des Geschäfts und nach der Funktion der für die Bearbeitung zuständigen Person.

[3] Im Übrigen gilt die Allgemeine Gebührenverordnung vom 8. September 2004[3].

7. Kapitel: Schlussbestimmungen

Art. 46 Aufhebung und Änderung anderer Erlasse

Die Aufhebung und die Änderung anderer Erlasse werden im Anhang 2 geregelt.

Art. 47 Übergangsbestimmung betreffend die Meldung geplanter automatisierter Bearbeitungstätigkeiten an den EDÖB

Artikel 32 ist nicht anwendbar auf geplante automatisierte Bearbeitungstätigkeiten, bei welchen im Zeitpunkt des Inkrafttretens die Projektfreigabe oder der Entscheid zur Projektentwicklung bereits erfolgt ist.

Art. 48 Inkrafttreten

Diese Verordnung tritt am ... in Kraft.

… Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Guy Parmelin
Der Bundeskanzler: Walter Thurnherr

[3] SR **172.041.1**

Anhang 1
(Artikel 8 Absatz 5)

Staaten, Gebiete, spezifische Sektoren in einem Staat und internationale Organe mit einem angemessenen Datenschutz

Andorra	Liechtenstein
Argentinien	Litauen
Belgien	Luxemburg
Bulgarien	Malta
Dänemark	Monaco
Deutschland	Neuseeland
Estland	Niederlande
Färöer	Norwegen
Finnland	Österreich
Frankreich	Polen
Gibraltar	Portugal
Griechenland	Rumänien
Guernsey	Schweden
Irland	Slowakei
Island	Slowenien
Isle of Man	Spanien
Israel	Tschechische Republik
Italien	Ungarn
Jersey	Uruguay
Kanada[4]	Vereinigtes Königreich[5]

[4] Ein angemessener Datenschutz wird gewährleistet, wenn das kanadische Bundesgesetz im privaten Bereich (The Personal Information Protection and Electronic Documents Act) oder das Gesetz einer Provinz zur Anwendung gelangt, das dem Bundesgesetz weitgehend entspricht. Das kanadische Bundesgesetz gilt für Personendaten, die im Rahmen kommerzieller Tätigkeiten beschafft, bearbeitet oder bekannt gegeben werden, unabhängig davon, ob es sich um Organisationen (z.B. Vereine, Personengesellschaften, Einzelpersonen und Gewerkschaften) oder bundesrechtlich geregelte Unternehmen (Anlagen, Werke, Unternehmen oder Geschäftstätigkeiten, die in die Gesetzgebungskompetenz des kanadischen Parlaments fallen) handelt. Folgende Provinzen haben ein Gesetz erlassen, das dem Bundesgesetz weitgehend entspricht: Québec, British Columbia und Alberta sowie Ontario, New Brunswick, Neufundland und Labrador und Neuschottland (für Gesundheitsdaten). Aber auch in diesen Provinzen gilt das Bundesgesetz wie im restlichen Kanada für alle Personendaten, die von bundesrechtlich geregelten Unternehmen beschafft, bearbeitet oder bekannt gegeben werden, einschliesslich der Daten über Angestellte dieser Unternehmen. Das Bundesgesetz gilt auch für Personendaten, die im Rah-

Kroatien	Zypern
Lettland	

men kommerzieller Tätigkeiten in eine andere Provinz oder ein anderes Land übermittelt werden.

5 Der Entscheid des Bundesrats bezieht sich nur auf Datenbearbeitungen, die nicht in den Anwendungsbereich der Schengen-relevanten Richtlinie (EU) 2016/680 fallen. In den von der Richtlinie (EU) 2016/680 erfassten Bereiche wird die Gesetzgebung des Vereinigten Königreichs gemäss dem Durchführungsbeschluss der Kommission vom ... gemäss der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten im Vereinigten Königreich als angemessen anerkannt.