

Verordnung über den Datenschutz (Datenschutzverordnung, DSV)

vom 31. August 2022 (Stand am 15. September 2024)

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 Datenschutzgesetzes vom 25. September 2020¹ (DSG),

verordnet:

1. Kapitel: Allgemeine Bestimmungen

1. Abschnitt: Datensicherheit

Art. 1 Grundsätze

¹ Zur Gewährleistung einer angemessenen Datensicherheit müssen der Verantwortliche und der Auftragsbearbeiter den Schutzbedarf der Personendaten bestimmen und die im Hinblick auf das Risiko geeigneten technischen und organisatorischen Massnahmen festlegen.

² Der Schutzbedarf der Personendaten wird nach den folgenden Kriterien beurteilt:

- a. Art der bearbeiteten Daten;
- b. Zweck, Art, Umfang und Umstände der Bearbeitung.

³ Das Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person wird nach den folgenden Kriterien beurteilt:

- a. Ursachen des Risikos;
- b. hauptsächliche Gefahren;
- c. ergriffene oder vorgesehene Massnahmen, um das Risiko zu verringern;
- d. Wahrscheinlichkeit und Schwere einer Verletzung der Datensicherheit trotz der ergriffenen oder vorgesehenen Massnahmen.

⁴ Bei der Festlegung der technischen und organisatorischen Massnahmen werden zudem die folgenden Kriterien berücksichtigt:

- a. Stand der Technik;
- b. Implementierungskosten.

⁵ Der Schutzbedarf der Personendaten, das Risiko und die technischen und organisatorischen Massnahmen sind über die gesamte Bearbeitungsdauer hinweg zu überprüfen. Die Massnahmen sind nötigenfalls anzupassen.

Art. 2 Ziele

Der Verantwortliche und der Auftragsbearbeiter müssen technische und organisatorische Massnahmen treffen, damit die bearbeiteten Daten ihrem Schutzbedarf entsprechend:

- a. nur Berechtigten zugänglich sind (Vertraulichkeit);
- b. verfügbar sind, wenn sie benötigt werden (Verfügbarkeit);
- c. nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität);
- d. nachvollziehbar bearbeitet werden (Nachvollziehbarkeit).

Art. 3 Technische und organisatorische Massnahmen

¹ Um die Vertraulichkeit zu gewährleisten, müssen der Verantwortliche und der Auftragsbearbeiter geeignete Massnahmen treffen, damit:

- a. berechnigte Personen nur auf diejenigen Personendaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigen (Zugriffskontrolle);
- b. nur berechnigte Personen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden (Zugangskontrolle);
- c. unbefugte Personen automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung benutzen können (Benutzerkontrolle).

² Um die Verfügbarkeit und Integrität zu gewährleisten, müssen der Verantwortliche und der Auftragsbearbeiter geeignete Massnahmen treffen, damit:

- a. unbefugte Personen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten können (Datenträgerkontrolle);
- b. unbefugte Personen Personendaten im Speicher nicht speichern, lesen, ändern, löschen oder vernichten können (Speicherkontrolle);
- c. unbefugte Personen bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht lesen, kopieren, verändern, löschen oder vernichten können (Transportkontrolle);
- d. die Verfügbarkeit der Personendaten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können (Wiederherstellung);
- e. alle Funktionen des automatisierten Datenbearbeitungssystems zur Verfügung stehen (Verfügbarkeit), Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität);

- f. Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden (Systemicherheit).

³ Um die Nachvollziehbarkeit zu gewährleisten, müssen der Verantwortliche und der Auftragsbearbeiter geeignete Massnahmen treffen, damit:

- a. überprüft werden kann, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert werden (Eingabekontrolle);
- b. überprüft werden kann, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekanntgegeben werden (Bekanntgabekontrolle);
- c. Verletzungen der Datensicherheit rasch erkannt (Erkennung) und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können (Beseitigung).

Art. 4 Protokollierung

¹ Werden besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet oder wird ein Profiling mit hohem Risiko durchgeführt und können die präventiven Massnahmen den Datenschutz nicht gewährleisten, so müssen der private Verantwortliche und sein privater Auftragsbearbeiter zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten protokollieren. Eine Protokollierung muss insbesondere dann erfolgen, wenn sonst nachträglich nicht festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie beschafft oder bekanntgegeben wurden.

² Das verantwortliche Bundesorgan und sein Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten.

³ Bei Personendaten, welche allgemein öffentlich zugänglich sind, sind zumindest das Speichern, Verändern, Löschen und Vernichten der Daten zu protokollieren.

⁴ Die Protokollierung muss Aufschluss geben über die Identität der Person, die die Bearbeitung vorgenommen hat, die Art, das Datum und die Uhrzeit der Bearbeitung sowie gegebenenfalls die Identität der Empfängerin oder des Empfängers der Daten.

⁵ Die Protokolle müssen während mindestens einem Jahr getrennt vom System, in welchem die Personendaten bearbeitet werden, aufbewahrt werden. Sie dürfen ausschliesslich den Organen und Personen zugänglich sein, denen die Überprüfung der Anwendung der Datenschutzvorschriften oder die Wahrung oder Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegt, und dürfen nur für diesen Zweck verwendet werden.

Art. 5 Bearbeitungsreglement von privaten Personen

¹ Der private Verantwortliche und sein privater Auftragsbearbeiter müssen ein Reglement für automatisierte Bearbeitungen erstellen, wenn sie:

- a. besonders schützenswerte Personendaten in grossem Umfang bearbeiten; oder

b. ein Profiling mit hohem Risiko durchführen.

² Das Reglement muss insbesondere Angaben zur internen Organisation, zum Datenbearbeitungs- und Kontrollverfahren sowie zu den Massnahmen zur Gewährleistung der Datensicherheit enthalten.

³ Der private Verantwortliche und sein privater Auftragsbearbeiter müssen das Reglement regelmässig aktualisieren. Wurde eine Datenschutzberaterin oder ein Datenschutzberater ernannt, so muss dieser oder diesem das Reglement zur Verfügung gestellt werden.

Art. 6 Bearbeitungsreglement von Bundesorganen

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

- a. besonders schützenswerte Personendaten bearbeiten;
- b. ein Profiling durchführen;
- c. nach Artikel 34 Absatz 2 Buchstabe c DSG Personendaten bearbeiten;
- d. Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen Personendaten zugänglich machen;
- e. Datenbestände miteinander verknüpfen; oder
- f. mit anderen Bundesorganen zusammen ein Informationssystem betreiben oder Datenbestände bewirtschaften.

² Das Reglement muss insbesondere Angaben zur internen Organisation, zum Datenbearbeitungs- und Kontrollverfahren sowie zu den Massnahmen zur Gewährleistung der Datensicherheit enthalten.

³ Das verantwortliche Bundesorgan und sein Auftragsbearbeiter müssen das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater zur Verfügung stellen.

2. Abschnitt: Bearbeitung durch Auftragsbearbeiter

Art. 7

¹ Die vorgängige Genehmigung des Verantwortlichen, die dem Auftragsbearbeiter erlaubt, die Datenbearbeitung einem Dritten zu übertragen, kann spezifischer oder allgemeiner Art sein.

² Bei einer allgemeinen Genehmigung informiert der Auftragsbearbeiter den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Dritter. Der Verantwortliche kann Widerspruch gegen diese Änderung erheben.

3. Abschnitt: Bekanntgabe von Personendaten ins Ausland

Art. 8 Beurteilung der Angemessenheit des Datenschutzes eines Staates, eines Gebiets, eines spezifischen Sektors in einem Staat oder eines internationalen Organs

¹ Die Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organe mit einem angemessenen Datenschutz werden in Anhang 1 aufgeführt.

² Bei der Beurteilung, ob ein Staat, ein Gebiet, ein spezifischer Sektor in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, werden insbesondere die folgenden Kriterien berücksichtigt:

- a. die internationalen Verpflichtungen des Staates oder internationalen Organs, insbesondere im Bereich des Datenschutzes;
- b. die Rechtsstaatlichkeit und die Achtung der Menschenrechte;
- c. die geltende Gesetzgebung insbesondere 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 einer oder mehrerer unabhängiger Behörden, die im betreffenden Staat für den Datenschutz zuständig sind oder denen ein internationales Organ untersteht und die über ausreichende Befugnisse und Kompetenzen verfügen.

³ Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) wird bei jeder Beurteilung konsultiert. Die Einschätzungen von internationalen Organen oder ausländischen Behörden, die für den Datenschutz zuständig sind, können berücksichtigt werden.

⁴ Die Angemessenheit des Datenschutzes wird periodisch neu beurteilt.

⁵ Die Beurteilungen werden veröffentlicht.

⁶ Wenn die Beurteilung nach Absatz 4 oder andere Informationen zeigen, dass kein angemessener Datenschutz mehr gewährleistet ist, wird Anhang 1 geändert; dies hat keine Auswirkungen auf die bereits erfolgten Datenbekanntgaben.

Art. 9 Datenschutzklauseln und spezifische Garantien

¹ Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSGVO und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSGVO müssen mindestens die folgenden Punkte enthalten:

- a. die Anwendung der Grundsätze der Rechtmässigkeit, von Treu und Glauben, der Verhältnismässigkeit, der Transparenz, der Zweckbindung und der Richtigkeit;
- b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen Personen;
- c. die Art und den Zweck der Bekanntgabe von Personendaten;

- d. gegebenenfalls die Namen der Staaten oder internationalen Organe, in die oder denen Personendaten bekanntgegeben werden, sowie die Anforderungen an die Bekanntgabe;
- e. die Anforderungen an die Aufbewahrung, die Löschung und die Vernichtung von Personendaten;
- f. die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger;
- g. die Massnahmen zur Gewährleistung der Datensicherheit;
- h. die Pflicht, Verletzungen der Datensicherheit zu melden;
- i. falls die Empfängerinnen und Empfänger Verantwortliche sind: die Pflicht, die betroffenen Personen über die Bearbeitung zu informieren;
- j. die Rechte der betroffenen Person, insbesondere:
 1. das Auskunftsrecht und das Recht auf Datenherausgabe oder -übertragung,
 2. das Recht, der Datenbekanntgabe zu widersprechen,
 3. das Recht auf Berichtigung, Löschung oder Vernichtung ihrer Daten,
 4. das Recht, eine unabhängige Behörde um Rechtsschutz zu ersuchen.

² Der Verantwortliche und im Fall von Datenschutzklauseln in einem Vertrag der Auftragsbearbeiter müssen angemessene Massnahmen treffen, um sicherzustellen, dass die Empfängerin oder der Empfänger diese Klauseln 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, sofern 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.

Art. 10 Standarddatenschutzklauseln

¹ Gibt der Verantwortliche oder der Auftragsbearbeiter Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSGVO 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. Er teilt das Ergebnis der Prüfung der Standarddatenschutzklauseln, die ihm unterbreitet werden, innerhalb von 90 Tagen mit.

Art. 11 Verbindliche unternehmensinterne Datenschutzvorschriften

¹ Verbindliche unternehmensinterne Datenschutzvorschriften nach Artikel 16 Absatz 2 Buchstabe e DSGVO 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 Einhaltung der verbindlichen unternehmensinternen Datenschutzvorschriften.

³ Der EDÖB teilt das Ergebnis der Prüfung der verbindlichen unternehmensinternen Datenschutzvorschriften, die ihm unterbreitet werden, innerhalb von 90 Tagen mit.

Art. 12 Verhaltenskodizes und Zertifizierungen

¹ Personendaten dürfen ins Ausland bekanntgegeben werden, wenn ein Verhaltenskodex oder eine Zertifizierung einen geeigneten Datenschutz gewährleistet.

² Der Verhaltenskodex muss vorgängig dem EDÖB zur Genehmigung unterbreitet 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

Art. 13 Modalitäten der Informationspflicht

Der Verantwortliche muss der betroffenen Person die Information über die Beschaffung von Personendaten in präziser, transparenter, verständlicher und leicht zugänglicher Form mitteilen.

Art. 14 Aufbewahrung der Datenschutz-Folgenabschätzung

Der Verantwortliche muss die Datenschutz-Folgenabschätzung nach Beendigung der Datenbearbeitung mindestens zwei Jahren aufbewahren.

Art. 15 Meldung von Verletzungen der Datensicherheit

¹ Die Meldung einer Verletzung der Datensicherheit an den EDÖB muss folgende Angaben enthalten:

- a. die Art der Verletzung;
- b. soweit möglich den Zeitpunkt und die Dauer;

- c. soweit möglich die Kategorien und die ungefähre Anzahl der betroffenen Personendaten;
 - d. soweit möglich die Kategorien und die 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 und die Folgen, einschliesslich der allfälligen Risiken, zu mindern;
 - g. den Namen und die Kontaktdaten einer Ansprechperson.
- ² Ist es dem Verantwortlichen nicht möglich, alle Angaben gleichzeitig zu melden, so liefert er die fehlenden Angaben so rasch als möglich nach.
- ³ Ist der Verantwortliche verpflichtet, die betroffene Person zu informieren, so teilt er ihr in einfacher und verständlicher Sprache mindestens die Angaben nach Absatz 1 Buchstaben a und e–g mit.
- ⁴ Der Verantwortliche muss die Verletzungen dokumentieren. Die Dokumentation muss die mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten. Sie ist ab dem Zeitpunkt der Meldung nach Absatz 1 mindestens zwei Jahre aufzubewahren.

3. Kapitel: Rechte der betroffenen Person

1. Abschnitt: Auskunftsrecht

Art. 16 Modalitäten

- ¹ Wer vom Verantwortlichen Auskunft darüber verlangt, ob Personendaten über sie oder ihn bearbeitet werden, muss dies schriftlich tun. Ist der Verantwortliche einverstanden, so kann das Begehren auch mündlich mitgeteilt werden.
- ² Die Auskunftserteilung erfolgt schriftlich oder in der Form, in der die Daten vorliegen. Im Einvernehmen mit dem Verantwortlichen kann die betroffene Person ihre Daten an Ort und Stelle einsehen. Die Auskunft kann mündlich erteilt werden, wenn die betroffene Person einverstanden ist.
- ³ Das Auskunftsbegehren und die Auskunftserteilung können auf elektronischem Weg erfolgen.
- ⁴ Die Auskunft muss der betroffenen Person in einer verständlichen Form erteilt werden.
- ⁵ Der Verantwortliche muss angemessene Massnahmen treffen, um die betroffene Person zu identifizieren. Diese ist zur Mitwirkung verpflichtet.

Art. 17 Zuständigkeit

¹ Bearbeiten mehrere Verantwortliche Personendaten gemeinsam, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen.

² Betrifft das Begehren Daten, die von einem Auftragsbearbeiter bearbeitet werden, so unterstützt der Auftragsbearbeiter den Verantwortlichen bei der Erteilung der Auskunft, sofern er das Begehren nicht im Auftrag des Verantwortlichen beantwortet.

Art. 18 Frist

¹ Die Auskunft muss innerhalb von 30 Tagen seit dem Eingang des Begehrens erteilt werden.

² Kann die Auskunft nicht innerhalb von 30 Tagen erteilt werden, so muss der Verantwortliche die betroffene Person darüber informieren und ihr mitteilen, innerhalb welcher Frist die Auskunft erfolgt.

³ Verweigert der Verantwortliche die Auskunft, schränkt er sie ein oder schiebt er sie auf, so muss er dies innerhalb derselben Frist mitteilen.

Art. 19 Ausnahme von der Kostenlosigkeit

¹ Ist die Erteilung der Auskunft mit einem unverhältnismässigen Aufwand verbunden, so kann der Verantwortliche von der betroffenen Person verlangen, dass sie sich an den Kosten angemessen beteiligt.

² Die Beteiligung beträgt maximal 300 Franken.

³ Der Verantwortliche muss der betroffenen Person die Höhe der Beteiligung vor der Auskunftserteilung mitteilen. Bestätigt die betroffene Person das Gesuch nicht innerhalb von zehn Tagen, so gilt es als ohne Kostenfolge zurückgezogen. Die Frist nach Artikel 18 Absatz 1 beginnt nach Ablauf der zehntägigen Bedenkzeit zu laufen.

2. Abschnitt: Recht auf Datenherausgabe oder -übertragung

Art. 20 Umfang des Anspruchs

¹ Als Personendaten, die die betroffene Person dem Verantwortlichen bekanntgegeben hat, gelten:

- a. Daten, die sie diesem wissentlich und willentlich zur Verfügung stellt;
- b. Daten, die der Verantwortliche über die betroffene Person und ihr Verhalten im Rahmen der Nutzung eines Diensts oder Geräts erhoben hat.

² Personendaten, die vom Verantwortlichen durch eigene Auswertung der bereitgestellten oder beobachteten Personendaten erzeugt werden, gelten nicht als Personendaten, die die betroffene Person dem Verantwortlichen bekannt gegeben hat.

Art. 21 Technische Anforderungen an die Umsetzung

¹ Als gängiges elektronisches Format gelten Formate, die es ermöglichen, dass die Personendaten mit verhältnismässigem Aufwand übertragen und von der betroffenen Person oder einem anderen Verantwortlichen weiterverwendet werden.

² Das Recht auf Datenherausgabe oder -übertragung begründet für den Verantwortlichen nicht die Pflicht, technisch kompatible Datenbearbeitungssysteme zu übernehmen oder beizubehalten.

³ Ein unverhältnismässiger Aufwand für die Übertragung von Personendaten auf einen anderen Verantwortlichen liegt vor, wenn die Übertragung technisch nicht möglich ist.

Art. 22 Frist, Modalitäten und Zuständigkeit

Die Artikel 16 Absätze 1 und 5 sowie 17–19 gelten sinngemäss für das Recht auf Datenherausgabe oder -übertragung.

4. Kapitel: Besondere Bestimmungen zur Datenbearbeitung durch private Personen

Art. 23 Datenschutzberaterin oder Datenschutzberater

Der 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 die Beraterin oder der Berater zur Erfüllung ihrer oder seiner Aufgaben benötigt;
- c. das Recht einräumen, in wichtigen Fällen das oberste Leitungs- oder Verwaltungsorgan zu informieren.

Art. 24 Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten

Unternehmen und andere privatrechtliche Organisationen, die am 1. Januar 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 besonders schützenswerte Personendaten in grossem Umfang bearbeitet.
- b. Es wird ein Profiling mit hohem Risiko durchgeführt.

5. Kapitel:

Besondere Bestimmungen zur Datenbearbeitung durch Bundesorgane

1. Abschnitt: Datenschutzberaterin oder -berater

Art. 25 Ernennung

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

Art. 26 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 wirkt bei der Anwendung der Datenschutzvorschriften mit, indem sie oder er insbesondere:
 1. die Bearbeitung von Personendaten prüft und Korrekturmassnahmen empfiehlt, wenn eine Verletzung der Datenschutzvorschriften festgestellt wird,
 2. den Verantwortlichen bei der Erstellung der Datenschutz-Folgenabschätzung berät und deren Ausführung überprüft.
- b. Sie oder er dient als Anlaufstelle für die betroffenen Personen.
- c. Sie oder er schult und berät die Mitarbeitenden des Bundesorgans in Fragen des Datenschutzes.

Art. 27 Pflichten des Bundesorgans

¹ Das Bundesorgan hat gegenüber der Datenschutzberaterin oder dem Datenschutzberater folgende Pflichten:

- a. Es gewährt ihr oder ihm Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten, die sie oder er zur Erfüllung ihrer oder seiner Aufgaben benötigt.
- b. Es sorgt dafür, dass sie oder er über eine Verletzung der Datensicherheit informiert wird.

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

Art. 28 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: Informationspflichten**Art. 29** Informationspflicht bei der Bekanntgabe von Personendaten

Das Bundesorgan informiert die Empfängerin oder den Empfänger über die Aktualität, Zuverlässigkeit und Vollständigkeit der von ihm bekanntgegebenen Personendaten, soweit sich diese Informationen nicht aus den Daten selbst oder aus den Umständen ergeben.

Art. 30 Informationspflicht 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 darauf hin.

**3. Abschnitt:
Meldung der Projekte zur automatisierten Bearbeitung von Personendaten an den EDÖB****Art. 31**

¹ Das verantwortliche Bundesorgan meldet dem EDÖB die geplanten automatisierten Bearbeitungstätigkeiten im Zeitpunkt des Entscheids zur Projektentwicklung oder der Projektfreigabe.

² Die Meldung muss die Angaben nach Artikel 12 Absatz 2 Buchstaben a–d DSGVO sowie das voraussichtliche Datum des Beginns der Bearbeitungstätigkeiten enthalten.

³ Der EDÖB nimmt diese Meldung in das Register der Bearbeitungstätigkeiten auf.

⁴ Das verantwortliche Bundesorgan aktualisiert die Meldung beim Übergang in den produktiven Betrieb oder bei der Projekteinstellung.

4. Abschnitt: Pilotversuche**Art. 32** Unentbehrlichkeit des Pilotversuchs

Ein 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 einer Aufgabe erfordert, dass die Personendaten im Abrufverfahren zugänglich sind.

Art. 33 Verfahren bei der Bewilligung des Pilotversuchs

¹ Vor der Konsultation der interessierten Verwaltungseinheiten legt das für den Pilotversuch zuständige Bundesorgan dar, wie die Einhaltung der Voraussetzungen nach Artikel 35 DSG erfüllt werden soll, und lädt den EDÖB zur Stellungnahme ein.

² Der EDÖB nimmt zur Frage Stellung, ob die Bewilligungsvoraussetzungen nach Artikel 35 DSG erfüllt sind. Das 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 eine Bearbeitung nach Artikel 34 Absatz 2 DSG erfordert und dass eine Testphase vor dem Inkrafttreten des Gesetzes im formellen Sinn unentbehrlich ist;
- 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 Planung der verschiedenen Phasen des Pilotversuchs.

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

⁴ Das Bundesorgan informiert den EDÖB über jede wichtige Änderung, welche die Einhaltung der Voraussetzungen nach 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 automatisierte Datenbearbeitung wird in einer Verordnung geregelt.

Art. 34 Evaluationsbericht

¹ Das zuständige Bundesorgan unterbreitet dem EDÖB den Entwurf des Evaluationsberichts an den Bundesrat zur Stellungnahme.

² Es unterbreitet dem Bundesrat den Evaluationsbericht mit der Stellungnahme des EDÖB.

5. Abschnitt: Datenbearbeitung für nicht personenbezogene Zwecke

Art. 35

Werden Personendaten zu nicht personenbezogenen Zwecken, insbesondere der Forschung, der Planung und der 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. 36 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 sind im Rahmen des Vorsorgewerks Bund bei der Pensionskasse des Bundes versichert.

Art. 37 Kommunikationsweg

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

² Der EDÖB reicht Berichte zuhanden der Bundesversammlung über die Parlamentsdienste ein.

Art. 38 Mitteilung von Entscheiden, Richtlinien und Projekten

¹ Die Departemente und die Bundeskanzlei teilen dem EDÖB im Bereich des Datenschutzes ihre Entscheide in anonymisierter Form sowie ihre Richtlinien 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. 39 Bearbeitung von Personendaten

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

- a. zur Ausübung seiner Aufsichtstätigkeiten;
- b. zur Ausübung seiner Beratungstätigkeiten;
- c. zur Zusammenarbeit mit Bundesbehörden, kantonalen und ausländischen Behörden;
- d. zur Aufgabenerfüllung im Rahmen der Strafbestimmungen nach dem DSG;

- e. zur Durchführung von Schlichtungsverfahren und zum Erlass von Empfehlungen nach dem Öffentlichkeitsgesetz vom 17. Dezember 2004² (BGÖ);
- f. zur Durchführung von Evaluationen nach dem BGÖ;
- g. zur Durchführung von Verfahren für den Zugang zu amtlichen Dokumenten nach dem BGÖ;
- h. zur Information der parlamentarischen Aufsicht;
- i. zur Information der Öffentlichkeit;
- j. zur Ausübung seiner Schulungstätigkeiten.

Art. 40 Selbstkontrolle

Der EDÖB erstellt ein Bearbeitungsreglement für sämtliche automatisierten Bearbeitungen; Artikel 6 Absatz 1 ist nicht anwendbar.

Art. 41³ Zusammenarbeit mit dem Bundesamt für Cybersicherheit

¹ Der EDÖB kann die Meldung einer Verletzung der Datensicherheit mit dem Einverständnis des meldepflichtigen Verantwortlichen zur Analyse des Vorfalls an das Bundesamt für Cybersicherheit (BACS) weiterleiten. Die Mitteilung kann Personendaten enthalten.

² Der EDÖB lädt das BACS zur Stellungnahme ein, bevor er anordnet, dass das Bundesorgan die Vorkehrungen nach Artikel 8 DSGVO trifft.

Art. 42 Register der Bearbeitungstätigkeiten der Bundesorgane

¹ Das Register der Bearbeitungstätigkeiten der Bundesorgane enthält die von den Bundesorganen gemachten Angaben nach Artikel 12 Absatz 2 DSGVO sowie nach Artikel 31 Absatz 2 dieser Verordnung.

² Es ist im Internet zu veröffentlichen. Nicht veröffentlicht werden die Registereinträge über geplante automatisierte Bearbeitungstätigkeiten nach Artikel 31.

Art. 43 Verhaltenskodizes

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

Art. 44 Gebühren

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

² SR 152.3

³ Fassung gemäss Ziff. II 7 der V vom 22. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS 2023 746).

² Es gilt ein Stundenansatz von 150 bis 250 Franken, je nach Funktion des ausführenden Personals.

³ Bei Dienstleistungen von aussergewöhnlichem Umfang, besonderer Schwierigkeit oder Dringlichkeit können Zuschläge bis zu 50 Prozent der Gebühr nach Absatz 2 erhoben werden.

⁴ Kann die Dienstleistung des EDÖB von der gebührenpflichtigen Person zu kommerziellen Zwecken weiterverwendet werden, so können Zuschläge bis zu 100 Prozent der Gebühr nach Absatz 2 erhoben werden.

⁵ Im Übrigen gilt die Allgemeine Gebührenverordnung vom 8. September 2004⁴.

7. Kapitel: Schlussbestimmungen

Art. 45 Aufhebung und Änderung anderer Erlasse

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

Art. 46 Übergangsbestimmungen

¹ Für Datenbearbeitungen, die nicht in den Anwendungsbereich der Richtlinie (EU) 2016/680⁵ fallen, gilt Artikel 4 Absatz 2 spätestens drei Jahre nach Inkrafttreten dieser Verordnung oder spätestens nach Ende des Lebenszyklus des Systems. In der Zwischenzeit unterliegen diese Bearbeitungen Artikel 4 Absatz 1.

² Artikel 8 Absatz 5 gilt nicht für Beurteilungen, die vor dem Inkrafttreten dieser Verordnung durchgeführt wurden.

³ Artikel 31 gilt nicht für geplante automatisierte Bearbeitungstätigkeiten, bei welchen im Zeitpunkt des Inkrafttretens dieser Verordnung die Projektfreigabe oder der Entscheid zur Projektentwicklung bereits erfolgt ist.

Art. 47 Inkrafttreten

Diese Verordnung tritt am 1. September 2023 in Kraft.

⁴ SR 172.041.1

⁵ Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, Fassung gemäss ABl. L 119 vom 4.5.2016, S. 89.

Anhang 1⁶
(Art. 8 Abs. 1)

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

- 1 Deutschland*
- 2 Andorra***
- 3 Argentinien***
- 4 Österreich*
- 5 Belgien*
- 6 Bulgarien***
- 7 Kanada***

Ein angemessener Datenschutz gilt als gewährleistet, wenn das kanadische Bundesgesetz «Loi sur la protection des renseignements personnels et les documents électroniques» vom 13. April 2000⁷ im privaten Bereich oder das Gesetz einer kanadischen Provinz, das diesem Bundesgesetz weitgehend entspricht, zur Anwendung gelangt. Das Bundesgesetz gilt für Personen­daten, die im Rahmen kommerzieller Tätigkeiten beschafft, bearbeitet oder bekanntgegeben werden, unabhängig davon, ob es sich um Organisationen wie Vereine, Personengesellschaften, Einzelpersonen oder Gewerkschaften oder bundesrechtlich geregelte Unternehmen wie Anlagen, Werke, Unternehmen oder Geschäftstätigkeiten, die in die Gesetzgebungskompetenz des kanadischen Parlaments fallen, handelt. Die Provinzen Québec, British Columbia und Alberta haben ein Gesetz erlassen, das dem Bundesgesetz weitgehend entspricht; die Provinzen Ontario, New Brunswick, Neufundland und Labrador und Neuschottland haben ein Gesetz erlassen, das im Bereich der Gesundheitsdaten diesem Gesetz weitgehend entspricht. In allen kanadischen Provinzen gilt das Bundesgesetz für alle Personendaten, die von bundesrechtlich geregelten Unternehmen beschafft, bearbeitet oder bekanntgegeben werden, einschliesslich der Daten über Angestellte dieser Unternehmen. Das Bundesgesetz gilt auch für Personendaten, die im Rahmen kommerzieller Tätigkeiten

⁶ Bereinigt gemäss Ziff. I der V vom 14. Aug. 2024, in Kraft seit 15. Sept. 2024 (AS 2024 435).

⁷ Der Text des kanadischen Bundesgesetzes ist abrufbar unter <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html>.

in eine andere Provinz oder in ein anderes Land über-
mittelt werden.

- 8 Zypern***
- 9 Kroatien***
- 10 Dänemark*
- 11 Spanien*
- 12 Estland*
- 13 Finnland*
- 14 Frankreich*
- 15 Gibraltar***
- 16 Griechenland*
- 17 Guernsey***
- 18 Ungarn*
- 19 Isle of Man***
- 20 Färöer***
- 21 Irland***
- 22 Island*
- 23 Israel***
- 24 Italien*
- 25 Jersey***
- 26 Lettland*
- 27 Liechtenstein*
- 28 Litauen*
- 29 Luxemburg*
- 30 Malta*
- 31 Monaco***
- 32 Norwegen*
- 33 Neuseeland***
- 34 Niederlande*
- 35 Polen*
- 36 Portugal*
- 37 Tschechien*
- 38 Rumänien***
- 39 Vereinigtes
Königreich**

- 40 Slowakei*
- 41 Slowenien*
- 42 Schweden*
- 43 Uruguay***
- 44 Vereinigte Staaten***

Für Personendaten, die von Organisationen bearbeitet werden, die gemäss den Grundsätzen des Datenschutzrahmens zwischen der Schweiz und den USA⁸ zertifiziert sind, gilt ein angemessenes Schutzniveau als gewährleistet, und zwar aufgrund der Garantien, die durch die Durchführungsverordnung 14086 vom 7. Oktober 2022⁹, die Vorschrift über das Gericht zur Datenschutzüberprüfung des Generalstaatsanwalts der Vereinigten Staaten vom 7. Oktober 2022¹⁰ und der Richtlinie 126 der Nachrichtendienstgemeinschaft (Verfahren für die Umsetzung für den Beschwerdemechanismus im Bereich der Nachrichtendienste gemäss Durchführungsverordnung 14086), die vom Büro der Direktorin des Nationalen Nachrichtendienstes am 6. Dezember 2022¹¹ erstellt wurde, gewährt werden sowie aufgrund der Ernennung der Schweiz am 7. Juni 2024¹² als Staat, der vom zweistufigen Beschwerdemechanismus einschliesslich des Zugangs zum Gericht zur Datenschutzüberprüfung profitiert.

- * Die Beurteilung der Angemessenheit des Datenschutzes schliesst die Bekanntgabe von Personendaten nach der Richtlinie (EU) 2016/680¹³ mit ein.
- ** Die Beurteilung der Angemessenheit des Datenschutzes schliesst die Bekanntgabe von Personendaten gemäss einem Durchführungsbeschluss der Europäischen Kommission, mit welchem die Angemessenheit des Datenschutzes nach der Richtlinie (EU) 2016/680 festgestellt wird, mit ein.
- *** Die Beurteilung der Angemessenheit des Datenschutzes schliesst die Bekanntgabe von Personendaten im Rahmen der von der Richtlinie (EU) 2016/680 vorgesehenen Zusammenarbeit nicht mit ein.

- ⁸ Die Grundsätze sind abrufbar unter: www.dataprivacyframework.gov/s/framework-text?tabset-c1491=3.
- ⁹ Das Exekutivdekret 14086 ist abrufbar unter: www.state.gov/executive-order-14086-policy-and-procedures/.
- ¹⁰ Die Vorschrift ist abrufbar unter: www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court.
- ¹¹ Die Richtlinie ist abrufbar unter: www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.
- ¹² Die Ernennung ist abrufbar unter: www.justice.gov/opcl/media/1355326/dl?inline.
- ¹³ Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, Fassung gemäss ABl. L 119 vom 4.5.2016, S. 89.

*Anhang 2*¹⁴
(Art. 45)

Aufhebung und Änderung anderer Erlasse

I

Die Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993¹⁵ wird aufgehoben.

II

Die nachstehenden Erlasse werden wie folgt geändert:

...¹⁶

¹⁴ Bereinigt gemäss Anhang 6 Ziff. II 1 der V vom 23. Sept. 2022 über genetische Untersuchungen beim Menschen, in Kraft seit 1 Sept. 2023 (AS **2022** 585).

¹⁵ [AS **1993** 1962; **2000** 1227 Anhang Ziff. II 7; **2006** 2331 Anhang 2 Ziff. 3, 4705 Ziff. II 24; **2007** 4993; **2008** 189; **2010** 3399]

¹⁶ Die Änderungen können unter AS **2022** 568 und AS **2022** 585 Anhang 6 Ziff. II 1 konsultiert werden.