Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

AS 2023
www.fedlex.admin.ch
Massgebend ist die signierte elektronische Fassung

Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee

(Informationssicherheitsverordnung, ISV)

vom 8. November 2023

Der Schweizerische Bundesrat,

gestützt auf die Artikel 2 Absätze 3 und 4, 12 Absatz 3, 83 Absatz 3, 84 Absatz 1, 85 Absätze 1 und 2 und 86 Absatz 4 des Informationssicherheitsgesetzes vom 18. Dezember 2020[1] (ISG),

verordnet:

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Gegenstand
(Art. 1 ISG)

Diese Verordnung regelt die Aufgaben, Verantwortlichkeiten und Kompetenzen sowie die Verfahren zur Gewährleistung der Informationssicherheit bei der Bundesverwaltung und der Armee.

Art. 2 Geltungsbereich
(Art. 2–3 ISG)

[1] Diese Verordnung gilt für:

a. den Bundesrat;

b. die Departemente;

c. die Bundeskanzlei (BK), die Generalsekretariate, die Gruppen und die Bundesämter;

d. die Armee.

SR **128.1**
1 SR **128**

2 Für Verwaltungseinheiten der dezentralen Bundesverwaltung nach Artikel 2 Absatz 3 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[2] (RVOG) und Organisationen nach Artikel 2 Absatz 4 RVOG gelten die folgenden Bestimmungen des ISG und der vorliegenden Verordnung:

a. wenn sie klassifizierte Informationen des Bundes bearbeiten: die Artikel 5–6, 9–10, 12–15, 20–23 und 27–73 ISG sowie die Artikel 16, 21, 24, 26 und 32, 34–35 dieser Verordnung;

b. wenn sie auf Informatikmittel der internen IKT-Leistungserbringer nach Artikel 9 der Verordnung vom 25. November 2020[3] über die digitale Transformation und die Informatik (VDTI) zugreifen oder ihre eigenen Informatikmittel durch diese Leistungserbringer betreiben lassen: die Artikel 5–6, 9–10, 16–73 ISG sowie die Artikel 10–12, 27 und 29–35 dieser Verordnung.

3 Die BK und die Departemente können in ihrem Zuständigkeitsbereich Verwaltungseinheiten der dezentralen Bundesverwaltung, die ständig sicherheitsempfindliche Tätigkeiten ausüben, dem gesamten ISG unterstellen.

4 Für die Kantone gelten unter Vorbehalt von Artikel 3 Absatz 2 ISG die folgenden Bestimmungen dieser Verordnung:

a. bei der Bearbeitung von klassifizierten Informationen des Bundes: die Bestimmungen des 4. Abschnitts;

b. beim Zugriff auf Informatikmittel des Bundes: die Artikel 28–30 und 34.

5 Die Gruppe Verteidigung übernimmt für die Armee die Aufgaben, Kompetenzen und Verantwortlichkeiten, die diese Verordnung den Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c zuweist.

2. Abschnitt: Grundsätze

Art. 3 Sicherheitsziele
(Art. 7 Abs. 2 Bst. a ISG)

1 Die Organisationen nach Artikel 2 Absatz 1 sorgen gemeinsam für einen risikobasierten Schutz ihrer Informationen und Informatikmittel sowie für eine angemessene Resilienz gegenüber Informationssicherheitsrisiken.

2 Sie tragen durch die Zusammenarbeit und den Informationsaustausch mit den anderen Bundesbehörden, den Kantonen, den Gemeinden, der Wirtschaft, der Gesellschaft, der Wissenschaft und den internationalen Partnern zur Verbesserung der Informationssicherheit der Schweiz bei.

3 Sie setzen sich für eine nationale und internationale Harmonisierung der Sicherheitsvorschriften und -niveaus ein, um die Interaktion von Bundesbehörden mit anderen Behörden des Bundes sowie den Kantonen, den Gemeinden und den internationalen Partnern zu ermöglichen.

2 SR **172.010**
3 SR **172.010.58**

Art. 4 Verantwortung

1 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c sind für den Schutz der Informationen, die sie bearbeiten oder deren Bearbeitung sie in Auftrag geben, sowie die Sicherheit der Informatikmittel, die sie selber betreiben oder durch Dritte betreiben lassen, verantwortlich.

2 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c nehmen in ihrem Zuständigkeitsbereich alle Aufgaben wahr, die diese Verordnung oder das übrige Bundesrecht nicht einer anderen Organisation oder Stelle zuweist.

3 Die Mitarbeitenden der Bundesverwaltung sowie die Angehörigen der Armee, die Informationen bearbeiten oder Informatikmittel des Bundes nutzen, sind für die vorschriftskonforme Bearbeitung und Nutzung verantwortlich.

4 Die Vorgesetzten aller Stufen sind für die aufgabenbezogene Schulung ihrer Mitarbeitenden beziehungsweise der ihnen unterstellten Angehörigen der Armee im Bereich der Informationssicherheit sowie für die Überprüfung der Einhaltung der Vorschriften durch diese verantwortlich.

3. Abschnitt: Management der Informationssicherheit

Art. 5 Informationssicherheits-Managementsystem
(Art. 7 Abs. 1 ISG)

1 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c erstellen je ein Informationssicherheits-Managementsystem (ISMS).

2 Sie legen die Ziele für ihr ISMS fest, prüfen jährlich, ob die Ziele erreicht werden, und erheben die dafür nötigen Kennzahlen.

3 Sie lassen ihr ISMS mindestens alle drei Jahre von einer unabhängigen Stelle oder ihrem Departement überprüfen und sorgen für die kontinuierliche Verbesserung des Systems.

4 Sie koordinieren ihr ISMS mit dem ordentlichen Risikomanagement, dem betrieblichen Kontinuitätsmanagement und dem Krisenmanagement.

Art. 6 Pflege der Rechtsgrundlagen und vertraglichen Verpflichtungen
(Art. 7 Abs. 1 ISG)

Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c, die Departemente und die Fachstelle des Bundes für Informationssicherheit führen je ein Verzeichnis der in ihrem Zuständigkeitsbereich massgebenden Rechtsgrundlagen und vertraglichen Verpflichtungen zur Informationssicherheit und halten es aktuell.

Art. 7 Inventarisierung der Schutzobjekte
(Art. 7 Abs. 1 ISG)

1 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c führen ein Inventar ihrer Schutzobjekte und halten es aktuell.

2 Als Schutzobjekte gelten einzelne oder mehrere gleichartige oder zusammenhängende:

a. Sammlungen von Informationen, die zur Abwicklung eines Geschäftsprozesses des Bundes bearbeitet werden;

b. Informatikmittel nach Artikel 5 Buchstabe a ISG.

3 Im Inventar ist festzuhalten:

a. der Schutzbedarf der Schutzobjekte;

b. die Verantwortlichkeiten für die Schutzobjekte;

c. die Beteiligung von Dritten;

d. das Ergebnis der Risikobeurteilung;

e. die Umsetzung der Sicherheitsmassnahmen und der Übernahme der Risiken, die nicht hinreichend reduziert werden können (Restrisiken);

f. die periodischen Kontrollen und Audits;

g. gegebenenfalls: die geteilte Nutzung der Schutzobjekte.

Art. 8 Risikomanagement
(Art. 7 Abs. 2 Bst. b und 8 ISG)

1 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c beurteilen laufend die Risiken für ihre Schutzobjekte und nehmen insbesondere folgende Aufgaben wahr:

a. Sie analysieren regelmässig Bedrohungen und Schwachstellen und bewerten deren Auswirkungen auf die Schutzobjekte.

b. Sie setzen die notwendigen Massnahmen um und kontrollieren die Wirkung.

c. Sie kontrollieren die Einhaltung der Vorgaben.

d. Sie weisen die Akzeptanz der Restrisiken nach.

2 Die Fachstelle des Bundes für Informationssicherheit, das Bundesamt für Cybersicherheit (BACS), die leistungserbringenden Verwaltungseinheiten und die Sicherheitsorgane des Bundes informieren die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c und die Departemente über aktuelle Bedrohungen und Schwachstellen sowie über Risiken, die sie betreffen. Sie empfehlen bei Bedarf Massnahmen zur Risikominderung.

3 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c berichten über ihre Informationssicherheitsrisiken im Rahmen des ordentlichen Risikomanagementprozesses nach den Vorgaben der Eidgenössischen Finanzverwaltung.

Art. 9 Bewilligung und Verzeichnung von Ausnahmen
(Art. 7 Abs. 1 ISG)

1 Kann eine Verwaltungseinheit für ein Schutzobjekt eine für sie verbindliche Vorgabe einer generell-abstrakten Weisung nach Artikel 85 ISG nicht erfüllen, so benötigt sie eine Ausnahmebewilligung der Stelle, welche die Weisungen erlassen hat.

2 Betrifft eine Ausnahme, die im Kompetenzbereich der Fachstelle des Bundes für Informationssicherheit liegt, auch Vorgaben der BK über die digitale Transformation und die IKT-Lenkung, so hört die Fachstelle des Bundes für Informationssicherheit vorgängig die DTI-Delegierte oder den DTI-Delegierten nach Artikel 4 Absatz 1 VDTI[4] an.

3 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c, die Departemente und die Fachstelle des Bundes für Informationssicherheit führen je ein Verzeichnis der gültigen Ausnahmebewilligungen.

Art. 10 Zusammenarbeit mit Dritten
(Art. 9 ISG)

1 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c beurteilen die Risiken für ihre Schutzobjekte bei der Zusammenarbeit mit Dritten und ihre Abhängigkeit von Dritten.

2 Die Beschaffungsstellen nach den Artikeln 9 und 10 der Verordnung vom 24. Oktober 2012[5] über die Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung (Org-VöB) wirken bei der Beurteilung mit und stellen die nötigen Informationen zur Verfügung.

3 Die Fachstelle des Bundes für Informationssicherheit empfiehlt nach Konsultation des BACS und der Beschaffungskonferenz des Bundes nach Artikel 24 Org-VöB, welche Bestimmungen zur Informationssicherheit in allen Beschaffungs- und Dienstleistungsverträgen des Bundes enthalten sein sollen.

Art. 11 Schulung und Sensibilisierung
(Art. 7 Abs. 1 und 20 Abs. 1 Bst. c ISG)

1 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c schulen ihre Mitarbeitenden bei Stellenantritt und anschliessend periodisch so, dass sie ihre Verantwortung in Bezug auf die Informationssicherheit wahrnehmen können. Sie führen ein Verzeichnis über die Schulungen und die Teilnahme daran.

2 Inhalt der Schulungen ist insbesondere:

a. die korrekte Identifizierung des Schutzbedarfs von Informationen;

b. der sichere Umgang mit Informationen und Informatikmitteln;

c. die korrekte Reaktion bei Verdacht auf einen Sicherheitsvorfall;

d. die Kenntnis der Sicherheitsorganisation sowie der Kontaktpersonen bei Fragen zur Informationssicherheit;

e. die Kontrollaufgaben der Vorgesetzten;

f. die Umsetzung der Informationssicherheit in Projekten und im Betrieb.

3 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c, die Departemente und die Fachstelle des Bundes für Informationssicherheit sorgen für die regelmässige

4 SR **172.010.58**
5 SR **172.056.15**

Sensibilisierung der Mitarbeitenden aller Stufen in Bezug auf die Risiken der Informationssicherheit.

4 Die Fachstelle des Bundes für Informationssicherheit erstellt Schulungs- und Sensibilisierungshilfsmittel.

Art. 12 Vorfallmanagement
(Art. 7 Abs. 1 und 10 Abs. 1 ISG)

1 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c legen in Absprache mit ihren Leistungserbringern fest, wie Sicherheitsvorfälle und Sicherheitslücken gemeldet und bewältigt beziehungsweise behandelt werden. Sie legen fest, wer Sofortmassnahmen anordnen kann.

2 Entdeckt ein Leistungserbringer Sicherheitsvorfälle oder Sicherheitslücken, die eine ihrer leistungsbeziehenden Verwaltungseinheiten betreffen, so meldet er ihr diese unverzüglich und unterstützt sie bei der Bewältigung beziehungsweise Behandlung.

3 Die Fachstelle des Bundes für Informationssicherheit und das BACS können die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c und die Departemente bei der Bewältigung von Sicherheitsvorfällen und der Behandlung von Sicherheitslücken unterstützen.

4 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c prüfen bei der Bewältigung von Sicherheitsvorfällen, ob eine Meldung nach der Datenschutzgesetzgebung an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten erfolgen muss.

5 Sie informieren ihr Departement und die Fachstelle des Bundes für Informationssicherheit unverzüglich über den Sicherheitsvorfall oder die Sicherheitslücke, wenn eine der folgenden Voraussetzungen erfüllt ist:

a. Die Funktionsfähigkeit der Bundesverwaltung könnte gefährdet sein.

b. Ein Informatikmittel der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz» ist betroffen.

c. Es könnten mehrere Departemente betroffen sein.

d. Der Schutz klassifizierter Informationen eines Staats oder einer internationalen Organisation, mit welchem oder welcher der Bundesrat einen völkerrechtlichen Vertrag nach Artikel 87 ISG abgeschlossen hat, könnte gefährdet sein.

e. Der Sicherheitsvorfall oder die Sicherheitslücke könnte eine hohe politische Bedeutung haben.

f. Der Sicherheitsvorfall oder die Sicherheitslücke erfordert Massnahmen ausserhalb des nach Absatz 1 festgelegten Verfahrens.

6 Die Fachstelle des Bundes für Informationssicherheit beurteilt mit der betroffenen Verwaltungseinheit das Risiko und den Unterstützungsbedarf.

7 Sie kann in Fällen nach Absatz 5 nach Rücksprache mit der betroffenen Verwaltungseinheit und dem betroffenen Departement die Federführung für die Bewältigung eines Sicherheitsvorfalls oder die Behandlung einer Sicherheitslücke übernehmen

oder diese mit deren Zustimmung dem BACS übertragen. Dabei haben sie folgende Aufgaben und Kompetenzen:

a. Sie können die betroffenen Verwaltungseinheiten, Leistungserbringer und Dritten verpflichten, ihr alle nötigen Informationen mitzuteilen.

b. Sie können Sofortmassnahmen anordnen.

c. Sie können externe Spezialistinnen und Spezialisten zur Unterstützung einsetzen.

d. Sie informieren die Leitung der betroffenen Verwaltungseinheiten und der Departemente über den Verlauf.

8 Ist nach einem Sicherheitsvorfall oder einer Sicherheitslücke die Informationssicherheit wiederhergestellt und sind die nötigen Folgearbeiten sowie deren Finanzierung definiert, so übergibt die Fachstelle des Bundes für Informationssicherheit oder das BACS die Federführung für die Weiterbearbeitung wieder der betroffenen Verwaltungseinheit.

Art. 13 Planung von Kontrollen und Audits

(Art. 7 Abs. 1, 81 Abs. 2 Bst. c und 83 Abs. 1 Bst. c ISG)

1 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c und die Departemente legen in je einem jährlichen Kontroll- und Auditplan fest, wie sie die Einhaltung der Vorschriften nach dieser Verordnung und die Wirksamkeit der Massnahmen zur Gewährleistung der Informationssicherheit in ihrem Zuständigkeitsbereich sowie bei beauftragten Dritten risikobasiert überprüfen.

2 Audits bei Dritten, die über eine Betriebssicherheitserklärung nach Artikel 61 ISG verfügen, müssen mit der Fachstelle Betriebssicherheit koordiniert werden.

3 Die Fachstelle des Bundes für Informationssicherheit erhebt den Kontroll- und Auditbedarf zur Gewährleistung der Informationssicherheit der gesamten Bundesverwaltung und der Armee.

4 Sie kann im Einvernehmen mit der BK oder dem zuständigen Departement Audits durchführen oder die Durchführung der Eidgenössischen Finanzkontrolle beantragen.

Art. 14 Berichterstattung

(Art. 7 Abs. 1, 81 Abs. 2 Bst. c und 83 Abs. 1 Bst. h ISG)

1 Die BK, die Departemente, das BACS und die internen IKT-Leistungserbringer nach Artikel 9 VDTI[6] erstatten der Fachstelle des Bundes für Informationssicherheit jährlich Bericht über den Stand der Informationssicherheit in ihrem Zuständigkeitsbereich. Sie erheben bei den Verwaltungseinheiten und ihren Leistungserbringern die dafür nötigen Informationen.

2 Die Fachstelle des Bundes für Informationssicherheit erstattet dem Bundesrat jährlich Bericht über den Stand der Informationssicherheit beim Bund.

6 SR **172.010.58**

3 Sie koordiniert die Berichterstattung mit den verpflichteten Behörden nach Artikel 2 Absatz 1 ISG.

Art. 15 Vorgaben zum Management der Informationssicherheit
(Art. 85 ISG)

Die Fachstelle des Bundes für Informationssicherheit erlässt generell-abstrakte Weisungen mit Geltung für alle Organisationen nach Artikel 2 Absätze 1 und 3 über die Mindestanforderungen an das Management der Informationssicherheit nach den Artikeln 5–14.

4. Abschnitt: Klassifizierte Informationen

Art. 16 Grundsätze
(Art. 11 und 14 ISG)

1 Die Bekanntgabe und das Zugänglichmachen klassifizierter Informationen sowie die Erstellung klassifizierter Informationsträger sind auf das Minimum zu beschränken.

2 Werden Informationen zu einem Sammelwerk zusammengefasst, ist die Klassifizierung neu zu beurteilen.

Art. 17 Klassifizierende Stellen
(Art. 12 ISG)

1 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c und die Departemente legen je in einem Klassifizierungskatalog fest, wie Informationen, die in ihrem Zuständigkeitsbereich häufig bearbeitet werden, zu klassifizieren sind und wie lange die Klassifizierung dauern soll.

2 Die Fachstelle des Bundes für Informationssicherheit überprüft die Klassifizierungskataloge und gibt bei Bedarf eine Empfehlung ab.

3 Sie legt nach der Konsultation der Konferenz der Informationssicherheitsbeauftragten in generell-abstrakten Weisungen mit Geltung für alle Organisationen nach Artikel 2 Absätze 1–3 fest, wie Informationen, die departementsübergreifend häufig bearbeitet werden, zu klassifizieren sind und wie lange die Klassifizierung dauern soll.

4 Folgende Personen und Stellen sind für die Klassifizierung und Entklassifizierung von Informationen, die nicht in den Klassifizierungskatalogen aufgeführt sind, zuständig:

a. die Mitarbeitenden des Bundes sowie die Angehörigen der Armee;

b. die Auftraggeberinnen, wenn Informationen des Bundes durch Dritte bearbeitet werden.

5 Die Mitarbeitenden des Bundes, die Angehörigen der Armee und die Dritten sind für die formelle Kennzeichnung der Informationsträger, die sie erstellen, oder der Informationen, die sie mündlich mitteilen, zuständig.

Art. 18 Klassifizierungsstufe «intern»
(Art. 13 Abs. 1 ISG)

1 Als «intern» werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte die Interessen nach Artikel 1 Absatz 2 Buchstaben a–d ISG wie folgt beeinträchtigen kann:

a. Ein wichtiger Geschäftsprozess des Bundesrats oder der Bundesverwaltung oder ein wichtiger Führungsprozess der Armee ist erschwert.

b. Die Durchführung von Einsätzen der Strafverfolgungsbehörden, des Nachrichtendiensts des Bundes (NDB), der Armee oder der anderen Sicherheitsorgane des Bundes ist erschwert.

c. Einzelne Personen sind körperlich verletzt.

d. Die nukleare Sicherheit oder die Sicherung von Kernanlagen und Kernmaterialien ist mittelbar gefährdet.

e. Die Schweiz ist aussenpolitisch oder wirtschaftlich benachteiligt.

f. Die Beziehungen zwischen Bund und Kantonen oder zwischen den Kantonen sind gestört.

2 Als «intern» werden zudem Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte Rückschlüsse auf «vertraulich» oder «geheim» klassifizierte Informationen ermöglichen.

Art. 19 Klassifizierungsstufe «vertraulich»
(Art. 13 Abs. 2 ISG)

Als «vertraulich» werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte die Interessen nach Artikel 1 Absatz 2 Buchstaben a–d ISG wie folgt erheblich beeinträchtigen kann:

a. Die Entscheidungs- oder Handlungsfähigkeit des Bundesrats, des Parlaments, mehrerer Verwaltungseinheiten oder mehrerer Truppenkörper der Armee ist über mehrere Tage erschwert.

b. Die zielkonforme Durchführung von Operationen der Strafverfolgungsbehörden, des NDB, der Armee oder der anderen Sicherheitsorgane des Bundes ist gefährdet.

c. Die operativen Mittel und Methoden der Nachrichtendienste und Strafverfolgungsbehörden des Bundes oder die Identität von Quellen und exponierten Personen sind offengelegt.

d. Die Sicherheit der Bevölkerung ist über mehrere Tage gefährdet oder einzelne Personen oder Personengruppen kommen zu Tode.

e. Die nukleare Sicherheit oder die Sicherung von Kernanlagen und Kernmaterialien ist gefährdet.

f. Die wirtschaftliche Landesversorgung oder der Betrieb von kritischen Infrastrukturen ist erschwert.

g. Die Schweiz ist aussenpolitisch oder wirtschaftlich erheblich benachteiligt oder die diplomatischen Beziehungen zu einem Staat oder zu einer internationalen Organisation sind abgebrochen.

h. Die Verhandlungsposition der Schweiz in wichtigen aussenpolitischen Geschäften ist vorübergehend erheblich geschwächt.

Art. 20 Klassifizierungsstufe «geheim»
(Art. 13 Abs. 3 ISG)

Als «geheim» werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte die Interessen nach Artikel 1 Absatz 2 Buchstaben a–d ISG wie folgt schwerwiegend beeinträchtigen kann:

a. Der Bundesrat, das Parlament, mehrere Verwaltungseinheiten oder mehrere Truppenkörper der Armee sind über Tage entscheidungs- oder handlungsunfähig oder ihre Entscheidungs- oder Handlungsfähigkeit ist über Wochen erschwert.

b. Die Durchführung von strategisch bedeutsamen Operationen der Strafverfolgungsbehörden, des NDB, der Armee oder der anderen Sicherheitsorgane des Bundes ist gefährdet oder über Tage in besonders hohem Mass erschwert.

c. Strategische Quellen, die Identität besonders exponierter Personen oder die strategischen Mittel und Methoden der Nachrichtendienste und Strafverfolgungsbehörden des Bundes sind offengelegt.

d. Die Sicherheit der Bevölkerung ist über Wochen in besonders hohem Mass gefährdet oder eine grosse Anzahl Personen kommt zu Tode.

e. Die nukleare Sicherheit oder die Sicherung von Kernanlagen und Kernmaterialien ist in besonders hohem Mass gefährdet.

f. Die wirtschaftliche Landesversorgung oder der Betrieb von kritischen Infrastrukturen fallen über Tage aus.

g. Die Schweiz leidet über Wochen unter besonders hohen aussenpolitischen oder wirtschaftlichen Konsequenzen wie Embargomassnahmen oder Sanktionen.

h. Die Verhandlungsposition der Schweiz in strategischen aussenpolitischen Geschäften ist über Jahre geschwächt.

Art. 21 Bearbeitungsvorgaben
(Art. 6 Abs. 2, 84 Abs. 1 und 85 ISG)

[1] Die Fachstelle des Bundes für Informationssicherheit erlässt generell-abstrakte Weisungen mit Geltung für alle Organisationen nach Artikel 2 Absätze 1–3 über die Bearbeitung klassifizierter Informationen und die organisatorischen, personellen, technischen und baulichen Mindestanforderungen für deren Schutz. Dabei trägt sie den einschlägigen internationalen Standards Rechnung.

2 Sie hört vorgängig die folgenden Stellen an:

a. das BACS;

b. den kryptografischen Dienst der Armee;

c. die für die Beschaffung von kryptologischen Gütern zuständigen Stellen nach Artikel 10 Absatz 1 Buchstabe d Org-VöB[7];

d. die für die Objektsicherheit zuständigen Stellen der Bundesverwaltung und der Armee.

3 Die BK regelt die Bearbeitung klassifizierter Bundesratsgeschäfte.

4 Die Bearbeitung klassifizierter Informationen aus dem Ausland erfolgt nach den Vorschriften, die der ausländischen Klassifizierungsstufe entsprechen. Vorbehalten bleiben abweichende Vorschriften eines völkerrechtlichen Vertrags nach Artikel 87 ISG.

Art. 22 Einsatzbezogene Sicherheitsmassnahmen
(Art. 6 Abs. 2 und 85 ISG)

1 Werden klassifizierte Informationen im Rahmen eines Einsatzes oder einer Operation bearbeitet und sind diese nur einem geschlossenen, eindeutig bestimmbaren Benutzerkreis zugänglich, so können die folgenden Personen nach Konsultation der Fachstelle des Bundes für Informationssicherheit einsatz- oder operationsspezifisch Vorschriften zur vereinfachten Bearbeitung beschliessen:

a. die Direktorin oder der Direktor des Bundesamts für Polizei;

b. die Direktorin oder der Direktor des NDB;

c. die Chefin oder der Chef der Armee;

d. die Chefin oder der Chef des Kommandos Operationen;

e. die Direktorin oder der Direktor des Bundesamts für Zoll und Grenzsicherheit.

2 Die Personen nach Absatz 1 sorgen dafür, dass auf den Informationsträgern eindeutig erkennbar ist, dass Vorschriften zur vereinfachten Bearbeitung gelten.

3 Ausserhalb des Benutzerkreises sowie für die Aufbewahrung im Hinblick auf die Archivierung gelten die Bearbeitungsvorgaben nach Artikel 21.

Art. 23 Sicherheitszertifizierung von Informatikmitteln
(83 Abs. 1 Bst. e ISG)

1 Informatikmittel müssen vor der Inbetriebnahme sicherheitsmässig zertifiziert werden, wenn dies für die nationale oder internationale Zusammenarbeit erforderlich ist.

2 Die Sicherheitszertifizierung erfolgt durch die Fachstelle des Bundes für Informationssicherheit nach Konsultation des kryptografischen Diensts der Armee sowie der für die Beschaffung von kryptologischen Gütern zuständigen Stellen nach Artikel 10 Absatz 1 Buchstabe d Org-VöB[8].

7 SR **172.056.15**
8 SR **172.056.15**

3 Sie belegt, dass das Informatikmittel die Mindestanforderungen für die entsprechende Klassifizierungsstufe erfüllt und die Restrisiken nach dem Stand der Technik tragbar sind.

4 Sie wird bei wesentlichen Änderungen der Risiken oder bei wesentlichen Änderungen am Informatikmittel wiederholt.

5 Das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) legt das Verfahren der Sicherheitszertifizierung fest und berücksichtigt dabei die einschlägigen internationalen Standards.

Art. 24 Schutz bei der Gefährdung von klassifizierten Informationen
(Art. 10 Abs. 1 und 11 Abs. 1 ISG)

1 Wer feststellt, dass klassifizierte Informationen gefährdet, abhandengekommen oder missbräuchlich verwendet worden sind oder Informationen offensichtlich falsch oder fälschlicherweise nicht klassifiziert sind, muss die nötigen Schutzmassnahmen treffen.

2 Sie oder er benachrichtigt unverzüglich die klassifizierende Stelle und die zuständigen Sicherheitsorgane.

Art. 25 Überprüfung von Schutzbedarf und Kreis der Berechtigten
(Art. 11 Abs. 2 ISG)

Die klassifizierenden Stellen überprüfen den Schutzbedarf ihrer klassifizierten Informationen und den Kreis der Berechtigten mindestens alle fünf Jahre sowie immer, wenn die Informationen dem Bundesarchiv zur Archivierung angeboten werden.

Art. 26 Archivierung
(Art. 12 Abs. 3 ISG)

1 Die Archivierung klassifizierter Informationen richtet sich nach den Vorschriften der Archivierungsgesetzgebung.

2 Das Bundesarchiv sorgt dafür, dass die Informationssicherheit nach dieser Verordnung gewährleistet ist.

3 Die Klassifizierung von Archivgut entfällt mit Ablauf der Schutzfrist. Verlängerungen der Schutzfrist richten sich nach Artikel 14 der Archivierungsverordnung vom 8. September 1999[9].

9 SR **152.11**

5. Abschnitt: Sicherheit beim Einsatz von Informatikmitteln

Art. 27 Sicherheitsverfahren
(Art. 16 ISG)

1 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c müssen den Schutzbedarf ihrer Schutzobjekte und deren Relevanz für das betriebliche Kontinuitätsmanagement nachweisen können.

2 Sie setzen die Mindestvorgaben der jeweiligen Sicherheitsstufe um und prüfen, ob zusätzliche Sicherheitsmassnahmen erforderlich sind.

3 Sie weisen Restrisiken aus.

4 Die Informationssicherheitsverantwortlichen (Art. 36) entscheiden, ob Restrisiken getragen werden. Sie können diesen Entscheid anderen Mitgliedern der Geschäftsleitung delegieren.

5 Das Sicherheitsverfahren wird bei wesentlichen Änderungen der Bedrohung, der Technologie, der Aufgaben oder der Organisationsverhältnisse wiederholt.

6 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c prüfen jährlich, ob eine wesentliche Änderung stattgefunden hat.

7 Die Fachstelle des Bundes für Informationssicherheit erlässt generell-abstrakte Weisungen mit Geltung für alle Organisationen nach Artikel 2 Absätze 1–3 über das Sicherheitsverfahren nach Artikel 16 ISG.

Art. 28 Zuordnung zu den Sicherheitsstufen «hoher Schutz» und «sehr hoher Schutz»
(Art. 17 ISG)

1 Die Sicherheitsstufe «hoher Schutz» wird einem Informatikmittel zugeordnet, wenn eine Verletzung der Informationssicherheit eine Beeinträchtigung nach Artikel 19 oder einen Schaden von fünfzig bis fünfhundert Millionen Franken zur Folge haben kann.

2 Die Sicherheitsstufe «sehr hoher Schutz» wird einem Informatikmittel zugeordnet, wenn eine Verletzung der Informationssicherheit eine Beeinträchtigung nach Artikel 20 oder einen Schaden über fünfhundert Millionen Franken zur Folge haben kann.

Art. 29 Sicherheitsmassnahmen
(Art. 6 Abs. 3, 18 und 85 ISG)

1 Die Fachstelle des Bundes für Informationssicherheit erlässt generell-abstrakte Weisungen mit Geltung für alle Organisationen nach Artikel 2 Absätze 1–3 über die Mindestanforderungen für die jeweiligen Sicherheitsstufen nach Artikel 17 ISG.

2 Sie berücksichtigt dabei die Anforderungen für die Sicherheit von Personendaten nach der Datenschutzgesetzgebung sowie von anderen Informationen, die der Bund aufgrund gesetzlicher oder vertraglicher Verpflichtungen schützen muss.

3 Bei den folgenden Informatikmitteln muss die Wirksamkeit der Sicherheitsmassnahmen vor der Inbetriebnahme, bei wesentlichen Änderungen der Risiken während des Betriebs, mindestens aber alle fünf Jahre überprüft werden:

a. Informatikmittel der Sicherheitsstufe «hoher Schutz», die für die Erfüllung behörden- oder departementsübergreifender Aufgaben eingesetzt werden;

b. Informatikmittel der Sicherheitsstufe «sehr hoher Schutz».

4 Die BK und die Departemente nehmen ihre Informatikmittel der Sicherheitsstufe «sehr hoher Schutz» in ihr Kontinuitätsmanagement auf.

Art. 30 Sicherheit beim Betrieb
(Art. 19 ISG)

1 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c stellen sicher, dass die Verantwortlichkeiten für die Informationssicherheit auf der betrieblichen Ebene in den Projekt- und Leistungsvereinbarungen mit den internen Leistungserbringern festgehalten sind.

2 Die internen Leistungserbringer stellen den Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c, den Departementen und der Fachstelle des Bundes für Informationssicherheit die Informationen zur Verfügung, welche diese für die Gewährleistung der Informationssicherheit benötigen.

3 Sie stellen sicher, dass sie über die nötigen personellen und finanziellen Kapazitäten und Fähigkeiten zur frühzeitigen Entdeckung, zur technischen Analyse und zur Bewältigung von Sicherheitsvorfällen und Behandlung von Sicherheitslücken verfügen, die sie selber oder, im Rahmen der Vereinbarungen nach Absatz 1, ihre Leistungsbezüger betreffen.

4 Sie überwachen die Nutzung ihrer Informatikinfrastruktur und durchsuchen sie regelmässig nach technischen Bedrohungen und Schwachstellen. Sie können Dritte mit der Durchsuchung beauftragen.

5 Die Bearbeitung von Personendaten im Rahmen der Überwachung und Durchsuchung nach Absatz 4 richtet sich nach der Verordnung vom 22. Februar 2012[10] über die Bearbeitung von Personendaten und Daten juristischer Personen bei der Nutzung der elektronischen Infrastruktur des Bundes.

6. Abschnitt: Personelle Massnahmen und physischer Schutz

Art. 31 Prüfung der Identität von Personen und Maschinen
(Art. 20 und 85 ISG)

1 Die Fachstelle des Bundes für Informationssicherheit kann nach Konsultation der oder des DTI-Delegierten generell-abstrakte Weisungen mit Geltung für alle Organisationen nach Artikel 2 Absätze 1–3 über die technischen Mindestanforderungen an die risikobasierte Prüfung der Identität von Personen und Maschinen, die Zugang zu

10 SR **172.010.442**

Informationen, Informatikmitteln, Räumlichkeiten und anderen Infrastrukturen des Bundes benötigen, erlassen.

2 Die Bearbeitung von Personendaten bei der Prüfung der Identität in Identitätsverwaltungs-Systemen nach Artikel 24 ISG richtet sich nach den Bestimmungen der Verordnung vom 19. Oktober 2016[11] über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes.

Art. 32 Personensicherheit
(Art. 6 Abs. 2 und 3, 8 sowie 20 Abs. 1 Bst. a und c ISG)

1 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c stellen sicher, dass Mitarbeitende, die einer Personensicherheitsprüfung nach der Verordnung vom 8. November 2023[12] über die Personensicherheitsprüfungen (VPSP) unterliegen, jährlich für die massgebende sicherheitsempfindliche Tätigkeit und die entsprechenden Risiken sensibilisiert werden.

2 Diese Mitarbeitende sind verpflichtet, ihrem Arbeitgeber Umstände aus ihrem privaten und beruflichen Umfeld, welche die vorschriftskonforme Ausübung der sicherheitsempfindlichen Tätigkeit gefährden können, zu melden.

Art. 33 Verdacht auf strafbares Verhalten
(Art. 7 Abs. 2 Bst. c ISG)

1 Kommt bei der Verletzung von Informationssicherheitsvorschriften zugleich eine strafbare Handlung in Betracht, überweisen die BK und die Departemente die Akten mit den Einvernahmeprotokollen der Bundesanwaltschaft oder dem Oberauditor der Schweizer Armee.

2 Sie stellen Gegenstände sicher, die geeignet sind, in einem Verfahren als Beweismittel zu dienen.

Art. 34 Physische Schutzmassnahmen
(Art. 22 und 85 ISG)

1 Die Fachstelle des Bundes für Informationssicherheit kann nach Konsultation der für die Objektsicherheit zuständigen Stellen der Bundesverwaltung und der Armee generell-abstrakte Weisungen mit Geltung für alle Organisationen nach Artikel 2 Absätze 1–3 über die Mindestanforderungen für den physischen Schutz von Informationen und Informatikmitteln erlassen.

2 Sie berücksichtigt dabei:

a. den gesamten Lebenszyklus der Informationen und Informatikmittel;

b. die arbeitsplatzspezifischen Anforderungen;

c. die Unterbringungsstrategien und -konzepte der Bundesverwaltung und der Armee.

11 SR **172.010.59**
12 SR **128.31**

Art. 35 Sicherheitszonen
(Art. 23 und 85 ISG)

1 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c können folgende Sicherheitszonen einrichten:

a. Sicherheitszone 1: Räumlichkeiten und Bereiche, in denen häufig als «vertraulich» klassifizierte Informationen bearbeitet oder Informatikmittel der Sicherheitsstufe «hoher Schutz» betrieben werden;

b. Sicherheitszone 2: Räumlichkeiten und Bereiche, in denen häufig als «geheim» klassifizierte Informationen bearbeitet oder Informatikmittel der Sicherheitsstufe «sehr hoher Schutz» betrieben werden.

2 Diese Räumlichkeiten und Bereiche gelten nur als Sicherheitszone, wenn die für die Objektsicherheit zuständige Stelle der Bundesverwaltung oder der Armee vor deren Inbetriebnahme und anschliessend mindestens alle fünf Jahre bestätigt, dass die Sicherheitsanforderungen erfüllt sind.

3 Die Fachstelle des Bundes für Informationssicherheit erlässt nach Konsultation der für die Objektsicherheit zuständigen Stellen der Bundesverwaltung und der Armee generell-abstrakte Weisungen mit Geltung für alle Organisationen nach Artikel 2 Absätze 1–3 über die Sicherheitsanforderungen für die Sicherheitszonen und deren Einrichtung.

4 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c können in der Umgebung von Sicherheitszonen Massnahmen zur Identifizierung von elektromagnetischen Ausspähungen und zum Schutz davor ergreifen.

7. Abschnitt: Sicherheitsorganisation

Art. 36 Informationssicherheitsverantwortliche der Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c
(Art. 7 Abs. 1 ISG)

1 Die Bundeskanzlerin oder der Bundeskanzler, die Generalsekretärinnen und Generalsekretäre sowie die Direktorinnen und Direktoren der Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c tragen in ihrem Zuständigkeitsbereich die Verantwortung für die Informationssicherheit.

2 Sie können die Informationssicherheitsverantwortung einem Mitglied der Geschäftsleitung delegieren, sofern diesem die erforderlichen Befugnisse zustehen, Massnahmen zu veranlassen, zu kontrollieren und zu korrigieren.

3 Die Informationssicherheitsverantwortlichen der Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c nehmen insbesondere folgende Aufgaben wahr:

a. Sie stellen den Aufbau, den Betrieb, die Überprüfung und die kontinuierliche Verbesserung des ISMS in ihrem Zuständigkeitsbereich sicher und erlassen die dafür nötigen Vorgaben.

b. Sie treffen alle Entscheide, welche die Informationssicherheit in ihrem Zuständigkeitsbereich massgeblich beeinflussen, insbesondere betreffend Organisation, Prozesse, Risikoakzeptanz und Sicherheitsziele.

c. Sie entscheiden über die erforderlichen Massnahmen, insbesondere über die Durchführung von Schulungs- und Sensibilisierungsmassnahmen.

d. Sie genehmigen den jährlichen Kontroll- und Auditplan und stellen die dafür nötigen Ressourcen zur Verfügung.

4 Die Bundeskanzlerin oder der Bundeskanzler, die Generalsekretärinnen und Generalsekretäre sowie die Direktorinnen und Direktoren der Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c beauftragen ihre Informationssicherheitsbeauftragten nach Artikel 37 und sorgen dafür, dass:

a. sie über angemessene Kompetenzen und Ressourcen verfügen; und

b. ihnen keine Aufgaben übertragen werden, die einen Interessenkonflikt mit den Aufgaben nach Artikel 37 zu Folgen haben können.

Art. 37 Informationssicherheitsbeauftragte der Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c
(Art. 7 Abs. 1 ISG)

1 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c bezeichnen eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten oder mehrere Informationssicherheitsbeauftragte sowie deren oder dessen Stellvertretung.

2 Die Informationssicherheitsbeauftragten haben insbesondere folgende Aufgaben und Kompetenzen:

a. Sie betreiben das ISMS der Verwaltungseinheit im Auftrag der oder des Informationssicherheitsverantwortlichen.

b. Sie erarbeiten die nötigen Entscheidgrundlagen zuhanden der oder des Informationssicherheitsverantwortlichen und beantragen ihr oder ihm den Beschluss von Massnahmen.

c. Sie sind die zentrale Anlaufstelle der Verwaltungseinheit für Fragen zur Informationssicherheit und beraten und unterstützen die zuständigen Personen und Stellen bei der Erfüllung ihrer Aufgaben und Pflichten im Bereich der Informationssicherheit.

d. Sie sorgen für die Umsetzung der Informationssicherheitsvorgaben und für die Anwendung des Sicherheitsverfahrens nach Artikel 27.

e. Sie beaufsichtigen das Verzeichnis der Rechtsgrundlagen, das Inventar der Schutzobjekte und das Verzeichnis der Ausnahmebewilligungen.

f. Sie beaufsichtigen die Planung der Schulung und Sensibilisierung nach Artikel 11 und beantragen der oder dem Informationssicherheitsverantwortlichen die Durchführung von zusätzlichen Schulungs- und Sensibilisierungsmassnahmen.

g. Sie stellen Antrag auf Einleitung des Betriebssicherheitsverfahrens nach Artikel 4 der Verordnung vom 8. November 2023[13] über das Betriebssicherheitsverfahren (VBSV).

h. Sie koordinieren die Bewältigung von Sicherheitsvorfällen und Behandlung von Sicherheitslücken in der Verwaltungseinheit sowie bei beauftragten Dritten.

i. Sie erstellen den jährlichen Kontroll- und Auditplan und unterbreiten ihn der oder dem Informationssicherheitsverantwortlichen zur Genehmigung.

j. Sie überprüfen periodisch das Vorhandensein und die Sicherheit von als «geheim» klassifizierten Informationsträgern in ihrem Zuständigkeitsbereich.

k. Sie können im Auftrag der oder des Informationssicherheitsverantwortlichen den Umgang mit Informationen an offenen, geteilten oder nicht abschliessbaren Arbeitsplätzen und in den Informatikmitteln der Verwaltungseinheit kontrollieren oder kontrollieren lassen.

l. Sie berichten der oder dem Informationssicherheitsverantwortlichen halbjährlich über den Stand der Informationssicherheit.

Art. 38 Informationssicherheit bei den Standarddiensten
(Art. 7 Abs. 1 ISG)

[1] Die oder der DTI-Delegierte ist für die Gewährleistung der Informationssicherheit bei den Standarddiensten nach Artikel 17 Absatz 1 Buchstabe e VDTI[14] zuständig.

[2] Sie oder er bezeichnet eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten oder mehrere Informationssicherheitsbeauftragte für die Standarddienste sowie deren oder dessen Stellvertretung.

[3] Die Informationssicherheitsbeauftragten nehmen für die Standarddienste die Aufgaben nach Artikel 37 Absatz 2 wahr und informieren die Bundesverwaltung und die Armee über die Informationssicherheitsrisiken.

Art. 39 Informationssicherheitsverantwortung der Departemente
(Art. 7 Abs. 1 und 81 ISG)

[1] Die Departemente sind für die Steuerung und Überwachung der Informationssicherheit in ihrem Zuständigkeitsbereich verantwortlich.

[2] Sie haben dabei insbesondere folgende Aufgaben:

a. Sie bestimmen die Informationssicherheitspolitik und die Sicherheitsorganisation des Departements, einschliesslich der fachlichen Führung der Informationssicherheitsbeauftragten nach Artikel 37.

b. Sie erlassen die nötigen Weisungen und überwachen die Umsetzung.

c. Sie überwachen die ISMS der Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c und erheben die dafür nötigen Kennzahlen.

13 SR **128.41**
14 SR **172.010.58**

d. Sie legen jährlich die Sicherheitsziele für die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c fest und überprüfen, ob sie erreicht wurden.

e. Sie genehmigen den jährlichen Kontroll- und Auditplan des Departements und stellen die nötigen Ressourcen zur Verfügung.

f. Sie beauftragen ihre Informationssicherheitsbeauftragten nach Artikel 40 und sorgen dafür, dass:

1. sie über angemessene Kompetenzen und Ressourcen verfügen;
2. ihnen keine Aufgaben übertragen werden, die einen Interessenkonflikt mit ihren Aufgaben nach Artikel 40 zur Folge haben können.

3 Sie können für ihren Zuständigkeitsbereich Sicherheitsanforderungen festlegen, die über die Mindestanforderungen der Fachstelle des Bundes für Informationssicherheit hinausgehen.

4 Sofern die Departementsvorsteherin oder der Departementsvorsteher nicht anders entscheidet, ist die Generalsekretärin oder der Generalsekretär in deren oder dessen Auftrag für die Informationssicherheit im Departement verantwortlich.

Art. 40 Informationssicherheitsbeauftragte der Departemente
(Art. 7 Abs. 1 und 81 ISG)

Die Informationssicherheitsbeauftragten der Departemente haben zusätzlich zu den Aufgaben nach Artikel 81 Absatz 2 ISG folgende Aufgaben:

a. Sie sorgen für die departementsübergreifende Koordination der Informationssicherheit.

b. Sie erarbeiten die nötigen Entscheidgrundlagen zuhanden der oder des Informationssicherheitsverantwortlichen und beantragen ihr oder ihm den Beschluss von Massnahmen.

c. Sie koordinieren die Bewältigung von Sicherheitsvorfällen und die Behandlung von Sicherheitslücken, welche mehrere Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c betreffen.

d. Sie erstellen den jährlichen Kontroll- und Auditplan des Departements und unterbreiten ihn der oder dem Informationssicherheitsverantwortlichen zur Genehmigung.

e. Sie vertreten das Departement in Fachgremien.

f. Sie werden bei der Wahl der Informationssicherheitsbeauftragten der Verwaltungseinheiten nach Artikel 37 konsultiert.

g. Sie kontrollieren periodisch sowie beim Wechsel oder beim Abgang eines Mitglieds des Bundesrats oder der Bundeskanzlerin oder des Bundeskanzlers, ob alle als «geheim» klassifizierten Informationsträger vollständig vorhanden sind.

h. Sie berichten der oder dem Informationssicherheitsverantwortlichen des Departements jährlich über den Stand der Informationssicherheit im Departement.

Art. 41 Informationssicherheitsbeauftragte oder -beauftragter des Bundesrates
(Art. 81 Abs. 1 Bst. a ISG)

Das VBS ernennt die Informationssicherheitsbeauftragte oder den Informationssicherheitsbeauftragten des Bundesrates sowie deren oder dessen Stellvertretung.

Art. 42 Fachstelle des Bundes für Informationssicherheit
(Art. 7 Abs. 1 und 83 ISG)

1 Die Fachstelle des Bundes für Informationssicherheit hat für die Bundesverwaltung und die Armee folgende Aufgaben und Kompetenzen:

a. Sie erarbeitet Strategien zu sicherheitsrelevanten Themen.

b. Sie kann bei sicherheitsrelevanten Vorhaben Informationen verlangen, dazu Stellung nehmen und Änderungen beantragen.

c. Sie wirkt bei der Ausbildung der Sicherheitsorganisation mit.

d. Sie stellt Vorlagen und Hilfsmittel bereit.

e. Sie unterstützt die Informationssicherheitsbeauftragten bei der Kontrolle der als «geheim» klassifizierten Informationsträger.

f. Sie verantwortet zertifizierte Sicherheitslösungen, die für die gesamte Bundesverwaltung und die Armee eingesetzt werden.

2 Sie konsultiert bei der Erfüllung dieser Aufgaben sowie den Aufgaben nach Artikel 83 Absatz 1 ISG die Konferenz der Informationssicherheitsbeauftragten.

3 Sie vertritt im internationalen Verhältnis als nationale Sicherheitsbehörde die Schweiz und nimmt dabei folgende Aufgaben wahr:

a. Sie erarbeitet die völkerrechtlichen Verträge nach Artikel 87 ISG und überwacht deren Umsetzung.

b. Sie stellt sicher, dass Sicherheitsvorfälle, die klassifizierte Informationen von Partnerstaaten betreffen, sachgerecht abgeklärt werden.

c. Sie führt die in den völkerrechtlichen Verträgen vorgesehenen Kontrollen durch oder gibt diese in Auftrag.

d. Sie vertritt die Schweiz in internationalen Fachgremien.

e. Sie bewilligt den Empfang von Personen aus dem Ausland, die für klassifizierte Projekte in die Schweiz reisen, sowie die Entsendung von Personen, die für klassifizierte Projekte ins Ausland reisen.

f. Sie stellt die Sicherheitsbescheinigungen nach Artikel 30 VPSP[15] aus.

4 Sie ist Teil des Staatssekretariats für Sicherheitspolitik im VBS.

15 SR **128.31**

Art. 43 Aufgaben und Kompetenzen des BACS
(Art. 7 Abs. 1 und 84 Abs. 1 ISG)

1 Das BACS hat folgende Aufgaben und Kompetenzen:

a. Es berät die Bundesverwaltung und die Armee sowie die Sicherheitsorgane nach den Artikeln 81–83 ISG in allen Belangen der technischen Informationssicherheit.

b. Es nimmt Einsitz in die Konferenz der Informationssicherheitsbeauftragten nach Artikel 82 ISG.

c. Es kann zur Beurteilung und Verbesserung des Stands der technischen Informationssicherheit des Bundes im Internet oder im Einvernehmen mit den jeweiligen Informationssicherheitsverantwortlichen und Leistungserbringern in der Informatikinfrastruktur der Bundesverwaltung nach technischen Bedrohungen und Schwachstellen suchen; es kann andere Stellen der Bundesverwaltung sowie Dritte damit beauftragen.

2 Es koordiniert seine Tätigkeiten mit der Fachstelle des Bundes für Informationssicherheit.

8. Abschnitt: Kosten und Evaluation

Art. 44 Kosten

1 Die dezentral anfallenden Kosten für die Informationssicherheit sind Teil der Projekt- und Betriebskosten.

2 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c stellen sicher, dass diese Kosten bei der Planung hinreichend berücksichtigt und ausgewiesen werden.

3 Für die Ausstellung und Zustellung von Sicherheitsbescheinigungen nach Artikel 30 VPSP[16] für Personen, die keine sicherheitsempfindliche Tätigkeit des Bundes erfüllen, erhebt die Fachstelle des Bundes für Informationssicherheit eine Gebühr von 100 Franken.

Art. 45 Evaluation
(Art. 88 ISG)

Die Fachstelle des Bundes für Informationssicherheit beantragt der Eidgenössischen Finanzkontrolle sechs Jahre nach Inkrafttreten dieser Verordnung und anschliessend alle zehn Jahre die Evaluation der Gesetzgebung über die Informationssicherheit beim Bund.

16 SR **128.31**

9. Abschnitt: Bearbeitung von Informationen und Personendaten

Art. 46 Allgemeines

1 Die Organisationen nach Artikel 2 Absätze 1–3 sowie die Sicherheitsorgane des Bundes können die für die Gewährleistung der Informationssicherheit zweckmässigen Informationen einschliesslich Personendaten bearbeiten.

2 Sie können untereinander sowie mit nationalen, internationalen und ausländischen Organisationen des öffentlichen und privaten Rechts Informationen einschliesslich Personendaten nach Absatz 1 austauschen, sofern:

a. dies zur Gewährleistung der Informationssicherheit zweckmässig ist;

b. keine gesetzlichen oder vertraglichen Geheimhaltungspflichten verletzt werden;

c. die Vorgaben der Bundesgesetzgebung über den Datenschutz eingehalten werden; und

d. diese Organisation gesetzliche Aufgaben im Bereich der Informationssicherheit wahrnehmen, die denjenigen der bekanntgebenden Behörde oder Organisation entsprechen.

3 Sofern dies für die Bewältigung eines Sicherheitsvorfalls oder die Behandlung einer Sicherheitslücke erforderlich ist, können sie auch besonders schützenswerte Personendaten nach Artikel 5 Buchstabe c des Datenschutzgesetzes vom 25. September 2020[17] von Personen, die daran beteiligt oder davon betroffen sind respektive sein könnten, bearbeiten und untereinander austauschen.

4 Werden bei einem Sicherheitsvorfall beim Bund oder bei Dritten, die mit dem Bund zusammenarbeiten, Informationen des Bundes entwendet und im Internet veröffentlicht, so dürfen sie die Informationen herunterladen und analysieren, um die Betroffenheit des Bundes zu beurteilen und die nötigen Schutzmassnahmen zu ergreifen. Sie dürfen Daten, die für die Beurteilung nicht relevant sind, nicht bearbeiten.

5 Sie dürfen diese Massnahmen bereits bei Vorliegen eines konkreten Verdachts anwenden.

Art. 47 ISMS-Anwendung

1 Die Organisationen nach Artikel 2 Absätze 1–3 können für das Management der Informationssicherheit ein Informationssystem (ISMS-Anwendung) betreiben.

2 Sie können in der ISMS-Anwendung alle Informationen im Zusammenhang mit dem Management der Informationssicherheit nach dieser Verordnung sowie die besonders schützenswerten Personendaten nach Artikel 46 Absatz 3 bearbeiten.

3 Sie können ihre ISMS-Anwendungen miteinander verknüpfen und informationssicherheitsrelevante Informationen über automatisierte Schnittstellen austauschen.

17 SR **235.1**

Art. 48 Elektronische Formulardienste

[1] Die Fachstelle des Bundes für Informationssicherheit kann für die nachfolgenden Zwecke elektronische Formulardienste betreiben und sie mit ihrer ISMS-Anwendung verknüpfen:

a. zur Abwicklung der Reisen nach Artikel 42 Absatz 3 Buchstabe e;

b. zur Ausstellung und Zustellung von Sicherheitsbescheinigungen im internationalen Verhältnis nach Artikel 30 VPSP[18];

c. zur Ausstellung und Zustellung von internationalen Betriebssicherheitsbescheinigungen nach Artikel 66 ISG.

[2] Mit den Formulardiensten nach Absatz 1 können die Personendaten nach Anhang 1 bearbeitet werden. Diese Daten dürfen längstens zehn Jahre aufbewahrt werden.

[3] Die Organisationen nach Artikel 2 Absätze 1–3 können elektronische Formulardienste zur Meldung von Sicherheitsvorfällen und Sicherheitslücken betreiben und sie mit ihrer ISMS-Anwendung verknüpfen.

[4] Mit den Formulardiensten nach Absatz 3 können sie Personendaten, einschliesslich besonders schützenswerte Personendaten nach Artikel 46 Absatz 3, bearbeiten, sofern sie für die Bewältigung von Sicherheitsvorfällen und Behandlung von Sicherheitslücken erforderlich sind. Sie müssen unmittelbar nach ihrer Bekanntgabe über den Formulardienst gelöscht werden. Sie dürfen vor dem Versand der Meldung während höchstens 24 Stunden vorübergehend gespeichert werden.

10. Abschnitt: Schlussbestimmungen

Art. 49 Besondere Vollzugsbestimmungen

Das VBS kann bestimmte datierte Fassungen der generell-abstrakten Weisungen nach den Artikeln 17 Absatz 3, 21 Absatz 1, 29 Absatz 1 und 34 Absatz 1 für die Kantone als verbindlich erklären.

Art. 50 Aufhebung und Änderung anderer Erlasse

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

Art. 51 Übergangsbestimmungen

[1] Vor Inkrafttreten dieser Verordnung durch das Nationale Zentrum für Cybersicherheit (NCSC) erlassene Vorgaben zur Informatiksicherheit und bewilligte Ausnahmen gelten bis höchstens drei Jahre nach Inkrafttreten dieser Verordnung.

[2] Über Änderungen an Vorgaben und bewilligten Ausnahmen, die vor Inkrafttreten dieser Verordnung durch das NCSC erlassen worden sind, entscheidet entweder die Fachstelle des Bundes für Informationssicherheit oder das NCSC.

18 SR **128.31**

3 Vor Inkrafttreten dieser Verordnung durch die Generalsekretärenkonferenz oder durch die Koordinationsstelle für den Informationsschutz im Bund erlassene Vorgaben zum Informationsschutz gelten bis höchstens zwei Jahre nach Inkrafttreten dieser Verordnung.

4 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c müssen ihr ISMS (Art. 5) innert drei Jahren nach Inkrafttreten dieser Verordnung aufbauen.

5 Die Klassifizierungskataloge (Art. 17) müssen bis spätestens ein Jahr nach Inkrafttreten dieser Verordnung erstellt werden.

6 Bis zum 30. Juni 2025 nimmt das BACS die Aufgaben und Kompetenzen der Fachstelle des Bundes für Informationssicherheit nach den Artikeln 9 Absätze 2 und 3, 11 Absätze 3 und 4, 12 Absätze 3 und 6–8, 15, 27 Absatz 7, 29 Absatz 1 und 31 Absatz 1 wahr.

7 Weisungen, die das BACS in Anwendung von Absatz 6 erlässt, gelten bis höchstens zwei Jahre nach Inkrafttreten dieser Verordnung.

Art. 52 Inkrafttreten

Diese Verordnung tritt am 1. Januar 2024 in Kraft.

8. November 2023

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Alain Berset
Der Bundeskanzler: Walter Thurnherr

Anhang 1
(Art. 48)

Datenbearbeitung mit den elektronischen Formulardiensten

Mit den folgenden Formulardiensten dürfen nachstehende Personendaten bearbeitet werden:

1. Formulardienst für den Zweck nach Artikel 48 Absatz 1 Buchstabe a

a. Angaben zur Person:
   1. Namen und Vornamen*
   2. AHV-Nummer
   3. Anrede, Titel und Rang*
   4. Geburtsdatum*
   5. Heimatort und Geburtsort*
   6. Nationalitäten*
   7. Identitätskarten- und Passnummer sowie Ausstellungsort und Gültigkeit*

b. Angaben zur beruflichen oder militärischen Funktion der Person:
   1. Funktion in der Organisation oder in der Armee*
   2. berufliche Adresse, E-Mail-Adresse, Telefonnummer und weitere, insbesondere elektronische Kontaktdaten
   3. positiver Entscheid über die Personensicherheitsprüfung, Prüfstufe und Gültigkeitsdauer*

c. Angaben zur antragstellenden Organisation:
   1. Name, Adresse und Kontaktdaten der Organisation*
   2. Name und Vornamen der Bezugsperson
   3. Funktion der Bezugsperson in der Organisation oder in der Armee
   4. berufliche Adresse, E-Mail-Adresse, Telefonnummer und elektronische Kontaktdaten der Bezugsperson

d. Angaben zum Besuch:
   1. Name, Adresse, E-Mail-Adresse und Kontaktdaten der ausländischen Organisation *
   2. Grund des Besuchs*
   3. Sicherheitsstufe des Besuchs*
   4. Dauer des Besuchs*
   5. Grenzübertrittpunkte*
   6. Transportmittel*
   7. mitgeführtes Material, einschliesslich Waffen, Munition und Sprengstoffe, Fahrzeuge und sonstige Ausrüstung*

Angaben mit einem Asterisk (*) werden der ausländischen Sicherheitsbehörde kommuniziert.

2. Formulardienst für den Zweck nach Artikel 48 Absatz 1 Buchstabe b

a. Angaben zur Person:
   1. Namen und Vornamen
   2. AHV-Nummer
   3. Anrede, Titel und Rang
   4. Geburtsdatum
   5. Heimatort und Geburtsort
   6. Nationalitäten
   7. Identitätskarten- und Passnummer sowie Ausstellungsort und Gültigkeit

b. Angaben zur beruflichen oder militärischen Funktion der Person:
   1. Funktion in der Organisation oder in der Armee
   2. berufliche Adresse, E-Mail-Adresse, Telefonnummer und weitere, insbesondere elektronische Kontaktdaten
   3. positiver Entscheid über die Personensicherheitsprüfung, Prüfstufe und Gültigkeitsdauer

c. Angaben zur antragsstellenden Organisation:
   1. Name, Adresse, E-Mail-Adresse und Kontaktdaten der Organisation
   2. Name und Vornamen der Bezugsperson
   3. Funktion der Bezugsperson in der Organisation oder in der Armee
   4. Berufliche Adresse, E-Mail-Adresse und weitere, insbesondere elektronische Kontaktdaten der Bezugsperson
   5. Grund für die Erstellung der Bescheinigung

3. Formulardienst für den Zweck nach Artikel 48 Absatz 1 Buchstabe c

a. Angaben zum Betrieb:
   1. Vollständiger Name*
   2. Rechtsform*
   3. Unternehmens-Identifikationsnummer
   4. Adresse, E-Mail-Adresse und weitere, insbesondere elektronische Kontaktdaten*
   5. Sitz*
   6. Namen und Vornamen der Bezugsperson*
   7. Funktion der Bezugsperson im Betrieb
   8. berufliche Adresse, E-Mail-Adresse und weitere, insbesondere elektronische Kontaktdaten der Bezugsperson

b. Angaben zur Betriebssicherheitserklärung:
   1. Ausstellungsdatum und Gültigkeitsdauer*
   2. Anwendungsbereich und Auflagen*
   3. Höchste zugelassene Klassifizierungs- oder Sicherheitsstufe*

Angaben mit einem Asterisk (*) werden der ausländischen Sicherheitsbehörde kommuniziert.

4. Formulardienst nach Artikel 48 Absatz 3

a. Angaben zur meldenden Person:
   1. Namen und Vornamen
   2. Adresse, E-Mail-Adresse, Telefonnummer und weitere, insbesondere elektronische Kontaktdaten
   3. Funktion in der Organisation oder in der Armee
b. Angaben zum Schadensereignis und zur Schadenbemessung
c. Bild-, Ton- oder Videoaufnahmen des Vorfalls oder der Sicherheitslücke
d. Dokumente oder Dateien mit Bezug zum Vorfall oder zur Sicherheitslücke
e. Angaben zu allenfalls am Vorfall beteiligten Personen
f. Erste Abklärungen von Sachverständigen einschliesslich bereits getroffener Massnahmen

Anhang 2
(Art. 50)

Aufhebung und Änderung anderer Erlasse

I

Die Cyberrisikenverordnung vom 27. Mai 2020[19] wird aufgehoben.

II

Die nachstehenden Erlasse werden wie folgt geändert:

1. Verordnung vom 4. Dezember 2009[20] über verwaltungspolizeiliche Massnahmen des Bundesamtes für Polizei und über das Informationssystem HOOGAN

Art. 9 Abs. 7

7 Die Behörden nach Absatz 1 stellen sicher, dass die Datenschutz- und Informationssicherheitsbestimmungen eingehalten werden.

Art. 13 Abs. 1 Bst. b

1 Für die Gewährleistung der Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom 8. November 2023[21].

2. Verordnung vom 16. August 2017[22] über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes

Art. 13 Abs. 1 Bst. b und c

1 Für die Gewährleistung der Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom 8. November 2023[23];

c. *Aufgehoben*

19 AS **2020** 2107, 5871; **2021** 132
20 SR **120.52**
21 SR **128.1**
22 SR **121.2**
23 SR **128.1**

Art. 15 Datenübermittlung ausserhalb von SiLAN

Für die Übermittlung von Daten des NDB ausserhalb von SiLAN gelten die Bestimmungen der Informationssicherheitsverordnung vom 8. November 2023[24].

3. Verordnung vom 10. November 2021[25] über das Einreise- und Ausreisesystem

Art. 20 Abs. 2 Bst. b

[2] Die Datensicherheit für die Bundesbehörden richtet sich zudem nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[26].

4. Asylverordnung 3 vom 11. August 1999[27]

Art. 12 Bst. b

Die Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[28];

5. Visa-Informationssystem-Verordnung vom 18. Dezember 2013[29]

Art. 34 Bst. b

Die Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[30];

6. ZEMIS-Verordnung vom 12. April 2006[31]

Art. 17 Sachüberschrift und Abs. 1 Bst. b

Daten- und Informationssicherheit

[1] Die Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[32].

24 SR **128.1**
25 SR **142.206**
26 SR **128.1**
27 SR **142.314**
28 SR **128.1**
29 SR **142.512**
30 SR **128.1**
31 SR **142.513**
32 SR **128.1**

7. Verordnung vom 5. Dezember 2008[33] über das Immobilienmanagement und die Logistik des Bundes

Art. 41 Abs. 2 Bst. b

2 Das BBL erlässt Weisungen für den Bereich Logistik. Vorbehalten bleiben:

b. der Informationssicherheitsverordnung vom 8. November 2023[34].

8. GEVER-Verordnung vom 3. April 2019[35]

Art. 11 Bearbeitung von klassifizierten Informationen

1 Informationen, die nach Artikel 19 der Informationssicherheitsverordnung vom 8. November 2023[36] als VERTRAULICH klassifiziert sind, werden in Geschäftsverwaltungssystemen verschlüsselt.

2 Informationen, die nach Artikel 20 der Informationssicherheitsverordnung als GEHEIM klassifiziert sind, dürfen nicht in Geschäftsverwaltungssystemen bearbeitet werden.

9. Verordnung vom 22. Februar 2012[37] über die Bearbeitung von Personendaten und Daten juristischer Personen, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen

Art. 3 Sichere Aufbewahrung

Die Daten sind gemäss den Bestimmungen der Informationssicherheitsverordnung vom 8. November 2023[38] sicher aufzubewahren.

33 SR **172.010.21**
34 SR **128.1**
35 SR **172.010.441**
36 SR **128.1**
37 SR **172.010.442**
38 SR **128.1**

10. IVIPS-Verordnung vom 18. November 2015[39]

Gliederungstitel vor Art. 10

3. Abschnitt: Datenschutz und Informationssicherheit

Art. 11 Abs. 1 Einleitungssatz und Bst. b

[1] Die Daten- und die Informationssicherheit richten sich nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[40].

11. Web-EDA-Verordnung vom 5. November 2014[41]

Gliederungstitel vor Art. 10

3. Abschnitt: Datenschutz und Informationssicherheit

Art. 12 Abs. 1 Einleitungssatz und Bst. b

[1] Die Daten- und die Informationssicherheit richten sich nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[42].

12. Verordnung E-VERA vom 17. August 2016[43]

Art. 14 Abs. 1 Einleitungssatz und Bst. b

[1] Die Daten- und Informationssicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[44];

39 SR **172.211.21**
40 SR **128.1**
41 SR **172.220.111.42**
42 SR **128.1**
43 SR **235.22**
44 SR **128.1**

13. Verordnung vom 7. November 2012[45] über den ausserprozessualen Zeugenschutz

Art. 4 Abs. 2

2 Im Übrigen gelten die Bestimmungen der Informationssicherheitsverordnung vom 8. November 2023[46].

Art. 12 Abs. 4

4 Für die Bearbeitung der Daten durch die empfangende Stelle oder Person gelten die Bestimmungen der Informationssicherheitsverordnung vom 8. November 2023[47].

Art. 15 Abs. 1 Bst. b

1 Für die Gewährleistung der Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom 8. November 2023[48];

14. Verordnung vom 20. September 2013[49] über das Informationssystem für Strafsachen des Bundesamts für Zoll und Grenzsicherheit

Art. 18 Abs. 1

1 Für die Gewährleistung der Datensicherheit gelten die Artikel 1–4 und 6 DSV[50] und die Bestimmungen der Informationssicherheitsverordnung vom 8. November 2023[51].

15. Strafregisterverordnung vom 19. Oktober 2022[52]

Art. 11 Abs. 1 Bst. b

1 Für die Gewährleistung der Datensicherheit gelten namentlich:

b. die Informationssicherheitsverordnung vom 8. November 2023[53].

45 SR **312.21**
46 SR **128.1**
47 SR **128.1**
48 SR **128.1**
49 SR **313.041**
50 SR **235.11**
51 SR **128.1**
52 SR **331**
53 SR **128.1**

16. ELPAG-Verordnung vom 23. September 2016[54]

Gliederungstitel vor Art. 13

6. Abschnitt: Richtigkeit der Daten, Informationssicherheit, Aufbewahrungsdauer, Archivierung und Statistik

Art. 14 Sachüberschrift sowie Abs. 1 Einleitungssatz und Bst. b

Daten- und Informationssicherheit

[1] Die Daten- und Informationssicherheit richten sich nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[55].

17. NES-Verordnung vom 15. Oktober 2008[56]

Art. 26 Bst. b

Für die Gewährleistung der Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom 8. November 2023[57] (ISV).

Art. 29n Abs. 1 Einleitungssatz (Betrifft nur den französischen Text) und Bst. b

[1] Für die Gewährleistung der Datensicherheit gelten:

b. die ISV[58].

Art. 29w Abs. 1 Einleitungssatz (Betrifft nur den französischen Text) und Bst. b

[1] Für die Gewährleistung der Datensicherheit gelten:

b. die ISV[59].

54 SR **351.12**
55 SR **128.1**
56 SR **360.2**
57 SR **128.1**
58 SR **128.1**
59 SR **128.1**

18. RIPOL-Verordnung vom 26. Oktober 2016[60]

Ersatz eines Ausdrucks

Im ganzen Erlass wird «Informatiksicherheit» *ersetzt durch* «Informationssicherheit».

Art. 9 Abs. 5

5 Die Bekanntgabe von Daten ist mit einem Hinweis zu versehen, wonach die Auskunft intern gemäss der Informationssicherheitsverordnung vom 8. November 2023[61] zu behandeln ist und nicht an weitere Interessierte weitergegeben werden darf.

Art. 14 Abs. 2 Bst. b

2 Die Datensicherheit richtet sich nach:

b. die Informationssicherheitsverordnung vom 8. November 2023[62].

19. IPAS-Verordnung vom 15. Oktober 2008[63]

Art. 12 Bst. b

Für die Gewährleistung der Datensicherheit gelten:

b. der Informationssicherheitsverordnung vom 8. November 2023[64].

20. Verordnung vom 6. Dezember 2013[65] über die Bearbeitung biometrischer erkennungsdienstlicher Daten

Art. 14 Bst. b

Die Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[66].

60 SR **361.0**
61 SR **128.1**
62 SR **128.1**
63 SR **361.2**
64 SR **128.1**
65 SR **361.3**
66 SR **128.1**

21. Polizeiindex-Verordnung vom 15. Oktober 2008[67]

Art. 12 Abs. 1 Bst. b

[1] Für die Gewährleistung der Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom 8. November 2023[68].

22. N-SIS-Verordnung vom 8. März 2013[69]

Art. 53 Abs. 1 Bst. b

[1] Die Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[70];

23. DNA-Profil-Verordnung vom 3. Dezember 2004[71]

Art. 19 Abs. 1 Bst. b

[1] Die Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[72].

24. Verordnung vom 15. September 2017[73] über die Informationssysteme im Berufsbildungs- und im Hochschulbereich

Art. 21 Abs. 1 Einleitungssatz und Bst. b

[1] Die Daten- und Informationssicherheit richten sich nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[74].

67 SR **361.4**
68 SR **128.1**
69 SR **362.0**
70 SR **128.1**
71 SR **363.1**
72 SR **128.1**
73 SR **412.108.1**
74 SR **128.1**

25. Verordnung vom 30. Juni 1993[75] über die Organisation der Bundesstatistik

Art. 10 Abs. 2

2 Für die Gewährleistung der Datensicherheit von Personendaten sowie von Daten juristischer Personen gelten neben den Bestimmungen des Gesetzes auch diejenigen der der Informationssicherheitsverordnung vom 8. November 2023[76] und der DSV. Für Daten juristischer Personen gilt die DSV sinngemäss.

26. Verordnung vom 9. Juni 2017[77] über das eidgenössische Gebäude- und Wohnungsregister

Art. 18 Abs. 1 Bst. b

1 Für die Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom 8. November 2023[78].

27. Verordnung vom 30. Juni 1993[79] über das Betriebs- und Unternehmensregister

Art. 15 Abs. 1 Bst. b

1 Für die Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom 8. November 2023[80].

28. Verordnung vom 20. April 2016[81] über die Kontrolle der rechtmässigen Herkunft von eingeführten Erzeugnissen der Meeresfischerei

Art. 24 Informationssicherheit

Die Massnahmen zur Gewährleistung der Informationssicherheit richten sich nach der Informationssicherheitsverordnung vom 8. November 2023[82].

75 SR **431.011**
76 SR **128.1**
77 SR **431.841**
78 SR **128.1**
79 SR **431.903**
80 SR **128.1**
81 SR **453.2**
82 SR **128.1**

29. Animex-ch-Verordnung vom 1. September 2010[83]

Ersatz eines Ausdrucks

Im ganzen Erlass wird «Informatiksicherheit» *ersetzt durch* «Informationssicherheit».

Art. 20 Abs. 1

[1] Die Massnahmen zur Gewährleistung der Informationssicherheit richten sich nach der Informationssicherheitsverordnung vom 8. November 2023[84].

30. Verordnung vom 24. Juni 2009[85] über internationale militärische Kontakte

Art. 4 Bst. c

Die folgenden Stellen dürfen in ihrem Aufgabenbereich ohne Bewilligung des Militärprotokolls internationale militärische Kontakte formell aufnehmen:

c. die Fachstelle des Bundes für Informationssicherheit;

Art. 5 Abs. 1

[1] Die Abgabe von klassifizierten Informationen an ausländische Personen und Stellen sowie der Zugang ausländischer Besucher und Besucherinnen zu klassifizierten militärischen Informationen, zu klassifiziertem Material oder zu militärischen Anlagen in der Schweiz richten sich nach den entsprechenden Informationsschutzvorschriften, insbesondere:

a. dem im konkreten Fall anwendbaren völkerrechtlichen Vertrag nach Artikel 87 des Informationssicherheitsgesetzes von 18. Dezember 2020[86];

b. der Verordnung vom 8. November 2023[87] über die Personensicherheitsprüfungen;

c. der Informationssicherheitsverordnung vom 8. November 2023[88];

d. der Verordnung über das Betriebssicherheitsverfahren vom 8. November 2023[89].

83 SR **455.61**
84 SR **128.1**
85 SR **510.215**
86 SR **128**
87 SR **128.31**
88 SR **128.1**
89 SR **128.41**

31. Verordnung vom 17. Oktober 2012[90] über die elektronische Kriegführung und die Funkaufklärung

Art. 7 Abs. 1

[1] Die Resultate der Funkaufklärungsaufträge werden nach der der Informationssicherheitsverordnung vom 8. November 2023[91] klassifiziert.

32. Waffenverordnung vom 2. Juli 2008[92]

Art. 66c Abs. 1 Bst. b

[1] Die Gewährleistung der Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[93].

33. Verordnung vom 12. August 2015[94] über die Meldestelle für lebenswichtige Humanarzneimittel

Art. 8 Abs. 2 Bst. b

[2] Im Übrigen gelten:

b. die Informationssicherheitsverordnung vom 8. November 2023[95].

34. Verordnung vom 19. August 2020[96] über die Sicherstellung der Trinkwasserversorgung in schweren Mangellagen

Art. 4 Abs. 5

[5] Das Inventar und die digitalen Karten werden nach Artikel 19 Buchstabe f der Informationssicherheitsverordnung vom 8. November 2023[97] (ISV) als VERTRAULICH klassifiziert.

Art. 7 Abs. 4

[4] Es wird nach Artikel 19 Buchstabe f ISV[98] als VERTRAULICH klassifiziert.

90 SR **510.292**
91 SR **128.1**
92 SR **514.541**
93 SR **128.1**
94 SR **531.215.32**
95 SR **128.1**
96 SR **531.32**
97 SR **128.1**
98 SR **128.1**

Art. 8 Abs. 5

5 Die Dokumentation wird nach Artikel 19 Buchstabe f ISV[99] als VERTRAULICH klassifiziert.

35. Datenbearbeitungsverordnung für das BAZG vom 23. August 2017[100]

Art. 12 Abs. 1

1 Für die Gewährleistung der Datensicherheit gelten die Artikel 1–4 und 6 der Datenschutzverordnung vom 31. August 2022[101] sowie die Informationssicherheitsverordnung vom 8. November 2023[102].

36. Energieverordnung vom 1. November 2017[103]

Art. 2 Abs. 2 Bst. d

2 Von diesen Pflichten ausgenommen sind Produzentinnen und Produzenten, deren Anlagen:

d. gemäss der Informationssicherheitsverordnung vom 8. November 2023[104] klassifiziert sind; oder

37. Organzuteilungsverordnung vom 16. März 2007[105]

Art. 34i Sachüberschrift und Abs. 1 Bst. b

Datensicherheit

1 Für die Gewährleistung der Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom 8. November 2023[106].

99 SR **128.1**
100 SR **631.061**
101 SR **235.11**
102 SR **128.1**
103 SR **730.01**
104 SR **128.1**
105 SR **810.212.4**
106 SR **128.1**

38. Verordnung vom 31. Oktober 2018[107] über das Informationssystem Antibiotika in der Veterinärmedizin

Art. 15 Informationssicherheit

Die Massnahmen zur Gewährleistung der Informationssicherheit richten sich nach der Informationssicherheitsverordnung vom 8. November 2023[108].

39. Verordnung vom 20. August 2014[109] über das Informationssystem des Zivildienstes

Art. 11 Abs. 1 Bst. b

1 Die Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[110];

40. Familienzulagenverordnung vom 31. Oktober 2007[111]

Art. 18h Sachüberschrift sowie Abs. 1 Einleitungssatz und Bst. b

Datenschutz und Informationssicherheit

1 Der Datenschutz und die Informationssicherheit richten sich nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[112];

41. Verordnung vom 18. November 2015[113] über die Ein-, Durch- und Ausfuhr von Tieren und Tierprodukten im Verkehr mit Drittstaaten

Art. 102g Informationssicherheit

Die Massnahmen zur Gewährleistung der Informationssicherheit richten sich nach der Informationssicherheitsverordnung vom 8. November 2023[114].

107 SR **812.214.4**
108 SR **128.1**
109 SR **824.095**
110 SR **128.1**
111 SR **836.21**
112 SR **128.1**
113 SR **916.443.10**
114 SR **128.1**

42. Verordnung vom 12. August 2015[115] über das Datenbearbeitungssystem private Sicherheitsdienstleistungen

Art. 9 Abs. 1 Einleitungssatz und Bst. b

[1] Die Daten- und die Informationssicherheit richten sich nach:

b. der Informationssicherheitsverordnung vom 8. November 2023[116].

43. Edelmetallkontrollverordnung vom 8. Mai 1934[117]

Art. 34e

Die Rechte der betroffenen Personen, insbesondere das Recht auf Auskunft, auf Berichtigung und auf Vernichtung der Daten, richten sich nach dem Bundesgesetz vom 25. September 2020[118] über den Datenschutz.

Art. 34g Abs. 1

[1] Für die Gewährleistung der Datensicherheit gelten die Artikel 1–4 und 6 der Datenschutzverordnung vom 31. August 2022[119] sowie die Informationssicherheitsverordnung vom 8. November 2023[120].

44. Sprengstoffverordnung vom 27. November 2000[121]

Art. 117j Abs. 1 Bst. b

[1] Für die Gewährleistung der Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom 8. November 2023[122].

115 SR **935.412**
116 SR **128.1**
117 SR **941.311**
118 SR **235.1**
119 SR **235.11**
120 SR **128.1**
121 SR **941.411**
122 SR **128.1**

45. Verordnung vom 25. August 2004[123] über die Meldestelle für Geldwäscherei

Art. 19 Abs. 1 Bst. b

[1] Für die Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom 8. November 2023[124].

123 SR **955.23**
124 SR **128.1**