Verordnung über die Informationssicherheit bei der Bundesverwaltung und bei der Armee

(Informationssicherheitsverordnung, ISV)

vom … Vorentwurf vom 24. August 2022

Der Schweizerische Bundesrat,

gestützt auf die Artikel 2 Abätze 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 und 84 Abs. 3 ISG)

[1] Diese Verordnung gilt für:

a. den Bundesrat;

b. die Verwaltungseinheiten der zentralen Bundesverwaltung nach Artikel 7 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[2] (RVOV);

c. die Armee.

[2] Das ISG und die vorliegende Verordnung gelten für Verwaltungseinheiten der dezentralen Bundesverwaltung nach Artikel 7*a* RVOV[3] wie folgt:

1 SR **128**
2 SR **172.010.1**
3 SR **172.010.1**

a. Für Verwaltungseinheiten, die auf Informatikmittel der internen IKT-Leistungserbringer nach Artikel 9 der Verordnung vom 25. November 2020[4] über die digitale Transformation und die Informatik (VDTI) zugreifen, sofern diese der Sicherheitsstufe «hohem Schutz» oder «sehr hohem Schutz» nach Artikel 28 zugeordnet sind: das gesamte ISG und die vorliegende Verordnung;

b. Für Verwaltungseinheiten, die Informatikmittel der Sicherheitsstufe «hohem Schutz» oder «sehr hohem Schutz» nach Artikel 28 einsetzen: das gesamte ISG und die vorliegende Verordnung;

c. Für Verwaltungseinheiten, die nicht unter Buchstaben a oder b fallen, die aber klassifizierte Informationen des Bundes bearbeiten: die Artikel 9–15 und 27–73 ISG sowie die Bestimmungen des 4. Abschnitts der vorliegenden Verordnung.

3 Die Bundeskanzlei oder die Departemente können beim Bundesrat beantragen, Verwaltungseinheiten der dezentralen Bundesverwaltung, die nicht unter Absatz 2 fallen, dem ISG und der vorliegenden Verordnung oder Teilen davon zu unterstellen.

4 Im Anhang 1 werden aufgeführt:

a. die Verwaltungseinheiten nach Absatz 2;

b. die Verwaltungseinheiten nach Absatz 3 und die jeweilige Geltung des ISG und der vorliegenden Verordnung.

5 Organisationen nach Artikel 2 Absatz 4 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[3] (RVOG) sind vom Geltungsbereich des ISG und der vorliegenden Verordnung ausgenommen.

6 Für die Kantone gelten unter Vorbehalt von Artikel 3 Absatz 2 ISG:

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.

2. Abschnitt: Grundsätze

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

1 Die Organisationen nach Artikel 2 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.

4 SR **172.010.58**

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 der Kantone und der Gemeinden zu ermöglichen.

Art. 4 Verantwortung

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

2 Die Verwaltungseinheiten nehmen in ihrem Zuständigkeitsbereich alle Aufgaben wahr, die diese Verordnung oder das 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 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 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 vom 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)

1 Die Verwaltungseinheiten, 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.

2 Die Verwaltungseinheiten und die Departemente konsultieren die Fachstelle des Bundes für Informationssicherheit bei sicherheitsrelevanten Vorgaben und Vorhaben.

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

1 Die Verwaltungseinheiten führen ein Inventar ihrer Schutzobjekte und halten es aktuell.

2 Als Schutzobjekte gelten:

a. Sammlungen von Informationen, die zur Erfüllung einer Aufgabe des Bundes bearbeitet werden;

b. Informatikmittel nach Artikel 5 Buchstabe a ISG.

3 Das Inventar dient dem Nachweis:

a. des Schutzbedarfs der Schutzobjekte;

b. der Verantwortlichkeiten für die Schutzobjekte;

c. gegebenenfalls der geteilten Nutzung der Schutzobjekte;

d. der Beteiligung von Dritten;

e. des Ergebnisses der Risikobeurteilung;

f. der Umsetzung der Sicherheitsmassnahmen und der Übernahme der Restrisiken;

g. der periodischen Kontrollen und Audits.

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

1 Die Verwaltungseinheiten beurteilen laufend die Risiken für ihre Schutzobjekte und nehmen dazu 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 die Akzeptanz der Restrisiken nach.

2 Die Fachstelle des Bundes für Informationssicherheit, die leistungserbringenden Verwaltungseinheiten und die Sicherheitsorgane des Bundes informieren die Verwaltungseinheiten und die Departemente über aktuelle Bedrohungen und Schwachstellen sowie über Risiken, die sie betreffen. Sie empfehlen bei Bedarf Massnahmen zur Risikominderung.

3 Die Verwaltungseinheiten 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 Vorgabe nicht erfüllen, so benötigt sie eine Bewilligung der Stelle, welche die Vorgabe beschlossen hat.

2 Die Fachstelle des Bundes für Informationssicherheit und die Departemente können die Bewilligung von Ausnahmen delegieren.

3 Betrifft eine Ausnahme, die im Kompetenzbereich der Fachstelle des Bundes für Informationssicherheit liegt, auch Vorgaben der Bundeskanzlei 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[5] an.

4 Die Verwaltungseinheiten, die Departemente und die Fachstelle des Bundes für Informationssicherheit führen je ein Verzeichnis der Ausnahmebewilligungen, die:

a. sie selber erteilt haben;

b. für ihre Schutzobjekte erteilt wurden.

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

1 Die Verwaltungseinheiten beurteilen nach den Vorgaben von Artikel 8 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[6] 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 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 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 sind insbesondere:

a. die korrekte Identifizierung des Schutzbedarfs von Informationen;

5 SR **172.010.58**
6 SR **172.056.15**

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, die Departemente und die Fachstelle des Bundes für Informationssicherheit sorgen für die regelmässige Sensibilisierung der Mitarbeitenden aller Stufen in Bezug auf die Risiken der Informationssicherheit.

4 Die Fachstelle des Bundes für Informationssicherheit stellt die Koordination sicher und erstellt Schulungs- und Sensibilisierungshilfsmittel.

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

1 Die Verwaltungseinheiten legen in Absprache mit ihren Leistungserbringern fest, wie Sicherheitsvorfälle und Sicherheitslücken gemeldet und bewältigt werden. Sie legen fest, wer über Sofortmassnahmen entscheidet.

2 Die Leistungserbringer melden ihren leistungsbeziehenden Verwaltungseinheiten unverzüglich entdeckte Sicherheitsvorfälle und Sicherheitslücken, die sie betreffen, und unterstützen sie bei der Bewältigung.

3 Die Fachstelle des Bundes für Informationssicherheit kann die Verwaltungseinheiten und die Departemente bei der Bewältigung von Sicherheitsvorfällen und der Behandlung von Sicherheitslücken unterstützen.

4 Die Verwaltungseinheiten 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 oder der Armee 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 Verfahrens nach Absatz 1.

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. Dabei hat sie folgende Aufgaben und Kompetenzen:

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

b. Sie kann Sofortmassnahmen anordnen.

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

d. Sie informiert 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 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 und die Departemente legen in 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 nach Artikel 51 Absatz 2 ISG koordiniert werden.

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

Art. 14 Berichterstattung

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

1 Die Departemente und die Bundeskanzlei erstatten der Fachstelle des Bundes für Informationssicherheit jährlich Bericht über den Stand der Informationssicherheit in ihrem Zuständigkeitsbereich.

2 Sie erheben bei den Verwaltungseinheiten und ihren Leistungserbringern die dafür nötigen Informationen.

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

4 Sie legt die Modalitäten der Berichterstattung der internen Leistungserbringer nach Artikel 9 VDTI[7] fest.

5 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 Stellen nach Artikel 2 Absätze 1–3 über die minimalen Anforderungen an das Management der Informationssicherheit nach den Artikeln 5–14.

4. Abschnitt: Klassifizierte Informationen

Art. 16 Grundsätze
(Art. 11 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 zu prüfen, ob dieses klassifiziert oder einer höheren Klassifizierungsstufe zugeordnet werden muss.

3 Bei Gesuchen um Zugang zu amtlichen Dokumenten überprüft die zuständige Stelle unabhängig von einem allfälligen Klassifizierungsvermerk, ob der Zugang nach dem Öffentlichkeitsgesetz vom 17. Dezember 2004[8] zu gewähren, zu beschränken, aufzuschieben oder zu verweigern ist.

Art. 17 Klassifizierende Stellen
(Art. 12 ISG)

1 Folgende Personen und Stellen sind für die Klassifizierung und Entklassifizierung von Informationen zuständig:

a. die Mitarbeitenden des Bundes sowie die Angehörigen der Armee: für Informationsträger, die sie erstellen oder erstellen lassen, und für Informationen, die sie mündlich mitteilen;

b. die Mitarbeitenden von Betrieben mit einer gültigen Betriebssicherheitserklärung nach Artikel 61 ISG: für Informationsträger, die sie im Auftrag des Bundes erstellen;

7 SR **172.010.58**
8 SR **152.3**

c. die für die Aufgabe verantwortliche Person: für Schutzobjekte nach Artikel 7 Absatz 2 Buchstabe a.

2 Die Verwaltungseinheiten, die Bundeskanzlei und die Departemente legen in einem Klassifizierungskatalog fest, wie Informationen, die in ihrem Zuständigkeitsbereich häufig bearbeitet werden, zu klassifizieren sind.

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

4 Sie legt nach der Konsultation der Konferenz der Informationssicherheitsbeauftragten fest, wie Informationen, die in der Bundesverwaltung und in der Armee häufig bearbeitet werden, zu klassifizieren sind.

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

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 über Monate gestört.

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 deren 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 Stellen nach Artikel 2 Absätze 1–3 über die Bearbeitung klassifizierter Informationen und die organisatorischen, personellen, technischen und baulichen Anforderungen für deren Schutz.

2 Sie hört vorgängig die folgenden Stellen an:

a. den kryptografischen Dienst der Armee;

b. die für die Beschaffung von kryptologischen Gütern zuständigen Stellen nach Artikel 10 Absatz 1 Buchstabe d Org-VöB[9]; und

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

3 Sie trägt den einschlägigen internationalen Standards Rechnung.

4 Die Bundeskanzlei regelt die Bearbeitung klassifizierter Bundesratsgeschäfte.

5 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 Stellen nach Absatz 1 sorgen dafür, dass eindeutig erkennbar ist, ob Vorschriften zur vereinfachten Bearbeitung gelten.

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

9 SR **172.056.15**

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

1 Informatikmittel müssen vor der Inbetriebnahme sicherheitsmässig akkreditiert werden, wenn eine der folgenden Voraussetzung erfüllt ist:

a. Sie werden für amtsübergreifende Aufgaben eingesetzt, bei denen als «geheim» klassifizierte Informationen bearbeitet werden.

b. Sie werden für behörden- oder departementsübergreifende Aufgaben eingesetzt, bei denen als «vertraulich» klassifizierte Informationen bearbeitet werden.

c. Die Sicherheitsakkreditierung ist für die nationale oder internationale Zusammenarbeit erforderlich.

2 Die Sicherheitsakkreditierung belegt, dass das Informatikmittel die minimalen Sicherheitsanforderungen für die entsprechende Klassifizierungsstufe erfüllt und die Restrisiken nach dem Stand der Technik tragbar sind.

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

4 Kann die Sicherheitsakkreditierung nicht erteilt werden, weil das Informatikmittel die minimalen Sicherheitsanforderungen nicht erfüllt, so entscheidet der Bundesrat über die Restrisiken.

5 Die Fachstelle des Bundes für Informationssicherheit nimmt folgende Aufgaben wahr:

a. Sie erteilt die Sicherheitsakkreditierung nach Konsultation des kryptografischen Diensts der Armee sowie der Stellen nach Artikel 10 Absatz 1 Buchstabe d Org-VöB[10].

b. Sie kann die Kompetenz zur Sicherheitsakkreditierung ausschliesslich militärischer Systeme der Gruppe Verteidigung delegieren.

6 Das [zuständige Departement] legt das Verfahren der Sicherheitsakkreditierung 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.

10 SR **172.056.15**

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. Eine Verlängerung der Schutzfrist richtet sich nach Artikel 14 der Archivierungsverordnung vom 8. September 1999[11].

5. Abschnitt: Sicherheit beim Einsatz von Informatikmitteln

Art. 27 Sicherheitsverfahren
(Art. 16 ISG)

[1] Die Verwaltungseinheiten 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 Risiken, die nicht hinreichend reduziert werden können (Restrisiken), aus.

[4] Die Sicherheitsverantwortlichen nach Artikel 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 prüfen jährlich, ob eine wesentliche Änderung nach Absatz 5 stattgefunden hat.

11 SR **152.11**

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 von mindestens 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 Stellen 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 Departemente und die Bundeskanzlei nehmen ihre Informatikmittel der Sicherheitsstufe «sehr hoher Schutz» in ihr Kontinuitätsmanagement auf.

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

[1] Die Verwaltungseinheiten 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, der Bundeskanzlei, 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 2, 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[12] über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen.

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 erlässt nach Konsultation der oder des DTI-Delegierten generell-abstrakte Weisungen mit Geltung für alle Stellen nach Artikel 2 Absätze 1–3 über die minimalen technischen Anforderungen an die risikobasierte Prüfung der Identität von Personen und Maschinen, die Zugang zu Informationen, Informatikmitteln, Räumlichkeiten und anderen Infrastrukturen des Bundes benötigen.

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[13] über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes.

Art. 32 Personensicherheit

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

1 Die Verwaltungseinheiten stellen sicher, dass Mitarbeitende, die einer Personensicherheitsprüfung nach der Verordnung vom …[14] über die Personensicherheitsprüfungen (VPSP) unterliegen, jährlich für die massgebende sicherheitsempfindliche Tätigkeit und die entsprechenden Risiken sensibilisiert werden.

2 Mitarbeitende nach Absatz 1 sind verpflichtet, ihrem Arbeitgeber Umstände aus ihrem privaten und beruflichen Umfeld, welche die vorschriftskonforme Ausübung der sicherheitsempfindlichen Tätigkeit gefährden, zu melden.

12 SR **172.010.442**
13 SR **172.010.59**
14 SR **128.xxx**

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 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 erlässt nach Konsultation der für die Objektsicherheit zuständigen Stellen der Bundesverwaltung und der Armee generell-abstrakte Weisungen mit Geltung für alle Stellen nach Artikel 2 Absätze 1–3 über die minimal erforderlichen Massnahmen zum physischen Schutz von Informationen und Informatikmitteln.

[2] Sie berücksichtigt dabei:

a. den gesamten Lebenszyklus der Informationen und Informatikmittel;

b. die arbeitsplatzspezifischen Anforderungen; und

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

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

[1] Die Verwaltungseinheiten 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] Die Räumlichkeiten und Bereiche nach Absatz 1 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 Stellen nach Artikel 2 Absätze 1–3 über die Sicherheitsanforderungen für die Sicherheitszonen und deren Einrichtung.

7. Abschnitt: Sicherheitsorganisation

Art. 36 Sicherheitsverantwortliche der Bundeskanzlei und der Verwaltungseinheiten
(Art. 7 Abs. 1 ISG)

1 Die Bundeskanzlerin oder der Bundeskanzler, die Generalsekretärinnen und Generalsekretäre sowie die Direktorinnen und Direktoren der Verwaltungseinheiten der zentralen und dezentralen Bundesverwaltung tragen in ihrem Zuständigkeitsbereich die Sicherheitsverantwortung.

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

3 Die Sicherheitsverantwortlichen der Bundeskanzlei und der Verwaltungseinheiten 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, Generalsekretärinnen und Generalsekretäre sowie die Direktorinnen und Direktoren der Verwaltungseinheiten der zentralen und dezentralen Bundesverwaltung 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
(Art. 7 Abs. 1 ISG)

1 Die Verwaltungseinheiten bezeichnen eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten oder mehrere Informationssicherheitsbeauftragte sowie deren oder dessen Stellvertretung.

2 Die Informationssicherheitsbeauftragten haben insbesondere folgende Aufgaben:

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

b. Sie erarbeiten die nötigen Entscheidgrundlagen zuhanden der oder des Sicherheitsverantwortlichen 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 Sicherheitsverantwortlichen die Durchführung von zusätzlichen Schulungs- und Sensibilisierungsmassnahmen.

g. Sie stellen Antrag auf Einleitung des Betriebssicherheitsverfahrens nach Artikel 4 der Verordnung über das Betriebssicherheitsverfahren vom …[15].

h. Sie koordinieren die Meldung und 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 Sicherheitsverantwortlichen zur Genehmigung.

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

k. Sie berichten der oder dem Sicherheitsverantwortlichen 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[16] zuständig.

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

[3] Die oder der Informationssicherheitsbeauftragte nimmt für die Standarddienste die Aufgaben nach Artikel 37 Absatz 2 wahr und informiert die Bundesverwaltung und die Armee über die Risiken.

15 SR **128.xxx**
16 SR **172.010.58**

Art. 39 Sicherheitsverantwortung 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 der Verwaltungseinheiten.

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

c. Sie überwachen die ISMS der Verwaltungseinheiten und erheben die dafür nötigen Kennzahlen.

d. Sie legen jährlich die Sicherheitsziele für die Verwaltungseinheiten fest und überprüfen, ob sie erreicht wurden.

e. Sie sorgen für eine risikobasierte Überprüfung der Informationssicherheit.

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 Aufgaben und Kompetenzen, welche diese Verordnung den Verwaltungseinheiten zuweist, übernehmen.

[4] Sie können für ihren Zuständigkeitsbereich Sicherheitsanforderungen festlegen, die über die Mindestanforderungen der Fachstelle des Bundes für Informationssicherheit oder der Verwaltungseinheit hinausgehen.

[5] Sofern die Departementsvorsteherin oder der Departementsvorsteher nicht anders entscheidet, ist die Generalsekretärin oder der Generalsekretär in deren oder dessen Auftrag für die Sicherheit 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 Sicherheitsverantwortlichen und beantragen ihr oder ihm den Beschluss von Massnahmen.

c. Sie koordinieren die Meldung und Bewältigung von Sicherheitsvorfällen und die Behandlung von Sicherheitslücken, welche mehrere Verwaltungseinheiten betreffen.

d. Sie vertreten das Departement in Fachgremien.

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

f. 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.

g. Sie bewilligen die Einleitung von Personensicherheitsprüfungen bei Dritten (Art. 8 Abs. 2 Bst. b VPSP[17]).

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

Art. 41 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:

a. Sie erarbeitet Strategien zu sicherheitsrelevanten Themen.

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

c. Sie wirkt bei der Ausbildung der Sicherheitsorganisation mit.

d. Sie stellt Vorlagen und Hilfsmittel bereit.

2 Sie kann zur Beurteilung und Verbesserung des Stands der Informationssicherheit des Bundes in der Informatikinfrastruktur der Bundesverwaltung und der Armee oder im Internet nach technischen Bedrohungen und Schwachstellen suchen; sie kann andere Stellen der Bundesverwaltung oder der Armee sowie Dritte damit beauftragen.

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

4 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 kann die in den völkerrechtlichen Verträgen vorgesehenen Kontrollen durchführen oder diese in Auftrag geben.

d. Sie vertritt die Schweiz in internationalen Fachgremien.

17 SR **128.xxx**

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 Bescheinigungen im internationalen Verhältnis nach Artikel 30 VPSP[18] aus.

5 Die Fachstelle des Bundes für Informationssicherheit ist dem *[zuständigen Departement]* zugeordnet.

8. Abschnitt: Kosten und Evaluation

Art. 42 Kosten

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

2 Die Verwaltungseinheiten stellen sicher, dass diese Kosten bei der Planung hinreichend berücksichtigt und ausgewiesen werden.

3 Für die Ausstellung und Zustellung von Sicherheitsbescheinigungen im internationalen Verhältnis nach Artikel 30 VPSP[19] für Personen, die keine sicherheitsempfindliche Tätigkeit des Bundes erfüllen, erhebt die Fachstelle des Bundes für Informationssicherheit eine Gebühr von 100 Franken.

Art. 43 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.

9. Abschnitt: Bearbeitung von Informationen und Personendaten

Art. 44 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. keine gesetzlichen oder vertraglichen Geheimhaltungspflichten verletzt werden; und

18 SR ...
19 SR **128.xxx**

b. die Vorgaben der Bundesgesetzgebung über den Datenschutz eingehalten werden.

3 Sofern dies für die Bewältigung eines Sicherheitsvorfalls oder einer Sicherheitslücke erforderlich ist, können sie auch besonders schützenswerte Personendaten über die Identität und die Handlungen von Personen, die am Vorfall beteiligt oder vom Vorfall betroffen sind oder sein könnten, bearbeiten und untereinander austauschen.

Art. 45 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 Daten nach Artikel 44 Absatz 3 bearbeiten.

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

Art. 46 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 41 Absatz 4 Buchstabe e;

b. zur Ausstellung und Zustellung von Sicherheitsbescheinigungen im internationalen Verhältnis nach Artikel 30 VPSP[20];

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

2 Mit den Formulardiensten nach Absatz 1 können die Personendaten nach Anhang 2 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 44 Absatz 3, die für die Bewältigung von Sicherheitsvorfällen und Sicherheitslücken erforderlich sind, bearbeiten.

5 Die Daten nach Absatz 4 müssen unmittelbar nach dem Versand der Meldung aus dem Formulardienst gelöscht werden. Sie dürfen vor dem Versand der Meldung während höchstens 24 Stunden vorübergehend gespeichert werden.

20 SR **128.xxx**

10. Abschnitt: Schlussbestimmungen

Art. 47 Aufhebung und Änderung anderer Erlasse

[1] Die folgenden Erlasse werden aufgehoben:

a. die Cyberrisikenverordnung vom 27. Mai 2020[21];

b. die Informationsschutzverordnung vom 4. Juli 2007[22].

[2] Die Änderung anderer Erlasse wird in Anhang 3 geregelt.

Art. 48 Übergangsbestimmungen

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

[2] Über Änderungen an Vorgaben und bewilligten Ausnahmen nach Absatz 1 entscheidet die Fachstelle des Bundes für Informationssicherheit.

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

[4] Die Verwaltungseinheiten und die Bundeskanzlei müssen ihr ISMS bis spätestens drei Jahre nach Inkrafttreten dieser Verordnung aufbauen.

[5] Die Sicherheitsakkreditierung nach Artikel 23 wird nicht durchgeführt bei Informatikmitteln, die:

a. vor Inkrafttreten dieser Verordnung in Betrieb sind;

b. bei Inkrafttreten dieser Verordnung in Entwicklung sind, sofern sie einen unverhältnismässig hohen Aufwand verursachen würde.

Art. 49 Inkrafttreten

Diese Verordnung tritt am … 2023 in Kraft.

… Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: …
Der Bundeskanzler: Walter Thurnherr

21 [AS **2020** 2107, **2020** 5871, **2021** 132]
22 [AS **2007** 3401, **2010** 3207, **2013** 1341, **2014** 3543, **2016** 1785, **2017** 7391, **2020** 6011]

Anhang 1
(Art. 2 Abs. 2 und 3)

Verwaltungseinheiten der dezentralen Bundesverwaltung, für welche die Informationssicherheitsverordnung gilt

1. Verwaltungseinheiten, die auf Informatikmittel der internen IKT-Leistungserbringer nach Artikel 9 VDTI[23] zugreifen, sofern diese der Sicherheitsstufe «hohem Schutz» oder «sehr hohem Schutz» nach Artikel 28 zugeordnet sind:

a. …
b. …
c. …

2. Verwaltungseinheiten, die Informatikmittel der Sicherheitsstufe «hohem Schutz» oder «sehr hohem Schutz» nach Artikel 28 einsetzen:

a. …
b. …
c. …

3. Verwaltungseinheiten, die nicht unter Artikel 2 Absatz 2 Buchstabe a oder b fallen, die aber klassifizierte Informationen des Bundes bearbeiten:

a. …
b. …
c. …

4. Weitere Verwaltungseinheiten (vgl. Art. 2 Abs. 3):

a. …
b. …
c. …

23 SR **172.010.58**

Anhang 2
(Art. 46 Abs. 2)

Datenbearbeitung in den elektronischen Formulardiensten nach Artikel 46

In den Formulardiensten nach Artikel 46 dürfen folgende Personendaten bearbeitet werden:

1. Formulardienst nach Artikel 46 Absatz 1 Buchstabe a ISV

   a. Angaben zur Person:
      1. Namen und Vornamen*
      2. AHV-Nummer
      3. Anrede, Titel und Rang*
      4. Geburtsdatum*
      5. Heimatort und Geburtsort*
      6. Nationalität/en*
      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 (*) werden der ausländischen Sicherheitsbehörde kommuniziert.

2. Formulardienst nach Artikel 46 Absatz 1 Buchstabe b ISV

   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 nach Artikel 46 Absatz 1 Buchstabe c ISV

   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 (*) werden der ausländischen Sicherheitsbehörde kommuniziert.

4. Formulardienst nach Artikel 46 Absätze 3–5 ISV

   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 3
(Art. 47 Abs. 2)

Änderung anderer Erlasse

Die nachstehenden Erlasse werden wie folgt geändert:

1. Verordnung vom 25. November 2020[24] über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung

Art. 2 Abs. 2 Einleitender Satz

2 Die nachstehenden Stellen können sich, unter dem Vorbehalt widersprechender organisationsrechtlicher Bestimmungen des Bundesrechts, durch eine Vereinbarung mit dem Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei (Bereich DTI der BK) verpflichten, diese Verordnung, die Informationssicherheitsverordnung vom […][25] und die GEVER-Verordnung vom 3. April 2019[26] einschliesslich der gestützt auf diese Verordnungen erlassenen Weisungen einzuhalten:

2. Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport vom 7. März 2003[27]

Art. 3 Abs. 2

2 Es erlässt Vorschriften zur Sicherstellung der Ausrüstung der Armee.

Art. 6 Bst. b

Aufgehoben

3. Verordnung vom 24. Juni 2009[28] über internationale militärische Kontakte

Art. 4 Bst. c

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

24 SR **172.010.58**
25 SR …
26 SR **172.010.441**
27 SR **172.214.1**
28 SR **510.215**

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 richtet sich nach den entsprechenden Informationsschutzvorschriften, insbesondere:

a. dem im konkreten Fall anwendbaren völkerrechtlichen Vertrag nach Artikel 87 des Informationssicherheitsgesetzes von 20. Dezember 2020[29];

b. der Verordnung vom …[30] über die Personensicherheitsprüfungen;

c. der Informationssicherheitsverordnung vom …[31];

d. der Verordnung über das Betriebssicherheitsverfahren vom …[32].

29 SR **128**
30 SR **...**
31 SR **...**
32 SR **...**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verordnung über die Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV)

Änderung vom … Entwurf vom 25. Juli 2022

Der Schweizerische Bundesrat
verordnet:

I

Die Verordnung vom 19. Oktober 2016[1] über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes wird wie folgt geändert:

Ingress

gestützt auf Artikel 26 und 84 Absatz 1 des Informationssicherheitsgesetzes vom 18. Dezember 2020[2] (ISG),
auf Artikel 27 Absätze 5 und 6 des Bundespersonalgesetzes vom 24. März 2000[3] und auf Artikel 186 des Bundesgesetzes vom 3. Oktober 2008[4] über die militärischen Informationssysteme,

Art. 2 Geltungsbereich

Diese Verordnung gilt für:

a. die Verwaltungseinheiten der zentralen Bundesverwaltung nach Artikel 7 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[5] (RVOV);

b. die Verwaltungseinheiten der dezentralen Bundesverwaltung nach Artikel 7*a* RVOV, sofern sie Zugriff auf Informatiksysteme der zentralen Bundesverwaltung haben.

1 SR **172.010.59**
2 SR **126**
3 SR **172.220.1**
4 SR **510.91**
5 SR **172.010.1**

Art. 3 Abs. 1

1 Der Zweck eines IAM-Systems ist es, Daten über die Identität und die Berechtigungen von Personen, Maschinen und Systemen gebündelt zu verwalten, um sie nachgelagerten Systemen und anderen IAM-Systemen zur Verfügung zu stellen.

Art. 5 IAM-Systeme

1 Die für IAM-Systeme verantwortlichen Bundesorgane sind:

a. der Bereich digitale Transformation und IKT-Lenkung der Bundeskanzlei (Bereich DTI der BK) für alle als Standarddienste angebotenen oder dem Bereich DTI der BK ausdrücklich zugewiesenen IAM-Systeme;

b. die Direktion für Ressourcen im Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) für das von der Informatik EDA betriebene IAM-System;

c. der Bereich DTI der BK für das IAM-System der Supportprozesse einschliesslich der Cloudanbindungen;

d. das Generalsekretariat des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport für das von der Führungsunterstützungsbasis (FUB) des VBS betriebene IAM-System;

e. das Generalsekretariat des Eidgenössischen Departements für Wirtschaft, Bildung und Forschung (WBF) für das beim Information Service Center WBF (ISCeco) betriebene IAM-System;

f. das Bundesamt für Strassen für sein IAM-System zum Betrieb der Betriebs- und Sicherheitsausrüstungen der Nationalstrassen.

2 Die Bundesorgane nach Absatz 1 sorgen dafür, dass die rechtmässige Bearbeitung der Personendaten in den IAM-Systemen, für die sie verantwortlich sind, mindestens alle vier Jahre von einer externen Stelle überprüft wird.

3 Sofern diese Verordnung auf die verpflichteten Behörden nach Artikel 2 Absatz 1 Buchstaben a und c–e ISG gemäss Artikel 84 Absatz 3 ISG anwendbar ist, legen diese selber fest, welches die in ihrem Bereich verantwortlichen Bundesorgane sind.

4 Die Verantwortung für das nachgelagerte System, insbesondere für den Zugang dazu, bleibt bei der zuständigen Fachstelle.

Art. 11 Abs. 2 und 3

2 Es darf in diesen Systemen kein Profiling durchgeführt werden.

3 Es dürfen in diesen Systemen, sofern hierfür keine besondere rechtliche Grundlage besteht, keine besonders schützenswerten Personendaten mit Ausnahme von biometrischen Daten nach Artikel 20 Absatz 2 ISG bearbeitet werden.

Art. 13 Abs. 4

4 Die Daten können weiteren bundesinternen Informationssystemen automatisch zur Übernahme und zum Abgleich bereitgestellt werden, sofern das jeweilige System:

a. über eine Rechtsgrundlage, welche die Bearbeitung der bereitzustellenden Daten vorsieht, und ein Bearbeitungsreglement nach Artikel 21 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG) verfügt; und

Art. 14 Abs. 2

2 Vorbehalten bleiben die Bestimmungen über die Vernichtung von biometrischen Daten nach Artikel 20 Absatz 2 ISG.

Gliederungstitel vor Art. 18

6. Abschnitt: Massnahmen zum Schutz der IAM-Systeme und Verzeichnisdienste

Art. 18 Abs. 1 und 2

1 Interne und externe Betreiber von Komponenten eines IAM-Systems oder Verzeichnisdiensts müssen über schriftlich festgehaltene Vorgaben für die Handhabung der Informationssicherheit und der Risiken verfügen. Insbesondere erlässt jedes verantwortliche Organ eines Systems oder Verzeichnisdiensts nach dieser Verordnung ein Bearbeitungsreglement nach Artikel 21 VDSG.

2 IAM-Systeme und Verzeichnisdienste, die nicht von Stellen nach Artikel 2 oder in deren Auftrag geführt werden, dürfen nur mit bundesinternen IAM-Systemen oder Verzeichnisdiensten verbunden werden, wenn sie die vordefinierten Minimalanforderungen bezüglich der Informationssicherheit erfüllen.

Art. 20 IAM-Gesamtsystem

Die IAM-Systeme der Bundesverwaltung können untereinander und mit den externen IAM-Systemen nach Artikel 21 zu einem Gesamtsystem verbunden werden.

Art. 21 Anschluss externer IAM-Systeme: Voraussetzungen

Die nachstehenden externen IAM-Systeme können für den Zugang der in ihnen geführten Personen zu den Ressourcen des Bundes an die IAM-Systeme des Bundes angeschlossen werden, sofern sie die Bedingungen und Verfahren nach den Artikeln 22 und 23 einhalten und ihre Betreiber sich verpflichten, diese Verordnung und die gestützt darauf erlassenen Vorgaben einzuhalten:

a. IAM-Systeme der Parlamentsdienste;

b. IAM-Systeme der Armee;

c. IAM-Systeme mit kantonalen und kommunalen Mitarbeiterinnen und Mitarbeitern nach Artikel 9 Buchstabe a;

d. vom Bereich DTI der BK anerkannte IAM-Systeme, die für den Identitätsverbund im E-Government vorgesehen sind;

e. ausländische IAM-Systeme oder Identitätsverbunde, deren gegenseitige Anbindung in einem Staatsvertrag vorgesehen ist; oder

f. Attribut-Register, die Angaben zu beruflichen Funktionen gemäss Anhang Buchstabe b für den Abruf bereitstellen.

II

Der Anhang erhält die neue Fassung gemäss Beilage.

III

Diese Verordnung tritt am … 2023 Kraft.

… Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: …
Der Bundeskanzler: Walter Thurnherr

Anhang
(Art. 11 und 13 Abs. 1 und 2)

Datenkategorien

Vorbemerkung: Zur Bedeutung der Sterne (*) siehe Artikel 11 Absatz 2.

	Verzeichnisdienste sowie IAM-Systeme mit Personen nach Art. 8 und 9 Bst. a	IAM-Systeme mit Personen nach Art. 9 Bst. b
a. Angaben zur Person		
1. Name*	x	x
2. Vornamen*	x	x
3. Geburtsdatum	x	x
4. Geschlecht	x	x
5. Anrede*	x	x
6. Titel*	x	x
7. Initialen*	x	x
8. lokale Personenidentifikatoren	x	x
9. Berufsbezeichnung*	x	x
10. Korrespondenzsprache*	x	x
11. besondere biometrische Personenmerkmale, insbesondere Irisbild, Retina, Venenscan, Fingerabdruck, Handabdruck, Gesichtsformmerkmale und Stimmprofil	x	
12. AHV-Nummer	x	x
b. Angaben zum Verhältnis zum Arbeit-/Auftraggeber		
1. Anstellungsverhältnis (intern/extern)*	x	
2. Informationen zur Organisation und zu den Planstellen*	x	x
3. künftige Zuordnung zu einer Organisationseinheit	x	
4. Personalkategorie	x	
5. Personalnummer (auch kantonale)	x	
6. Funktion*	x	
7. Stellenbezeichnung*	x	
8. Kennung des Personalinformationssystems (Quelle)	x	
9. Eintritts- und Austrittsdatum	x	
10. Ausweis- und/oder Badgenummer	x	x
c. Kontaktangaben		

	Verzeichnisdienste sowie IAM-Systeme mit Personen nach Art. 8 und 9 Bst. a	IAM-Systeme mit Personen nach Art. 9 Bst. b
1. Arbeitsort und geschäftliche Postadresse*	x	x
2. Büronummer*	x	
3. geschäftliche Adressierungselemente* wie E-Mail-Adresse*, Telefonnummern*, Faxnummer*, VOIP-Adresse*	x	x
4. externe Adressierungselemente* (für Mitarbeiter/innen und Beauftragte*) oder private Adressierungselemente	x	x
d. Angaben zu beruflichen Funktionen		
1. Einträge aus offiziellen Berufsregistern (Arzt/Ärztin, Urkundsperson, Anwalt/Anwältin usw.)	x	x
2. Funktionen gemäss Handelsregister und weiteren Vertretungsregistern	x	x
e. technische Angaben		
1. zugeordnete Geräte, Anschlüsse, Systeme, Anwendungen usw.	x	x
2. Adressierungselemente, Kennnummern usw.	x	
3. Systemsprache der Geräte, Anschlüsse usw.	x	x
4. öffentliche Schlüssel der digitalen Zertifikate*	x	x
5. Berechtigungsgruppen	x	x
6. Namen für die Anmeldung an den IT-Systemen	x	x
7. Passwörter	x	x
8. letztes Login	x	x
9. fehlgeschlagene Login-Versuche	x	x
10. Status (aktiv/passiv)	x	x
f. Daten über die Personensicherheitsprüfung, sofern diese zu einer vorbehaltlosen Sicherheitserklärung geführt hat oder die entscheidende Instanz einen positiven Entscheid gefällt hat		
1. Prüfstufe	x	
2. Geltungsdauer der Sicherheitserklärung	x	

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verordnung über die Personensicherheitsprüfungen (VPSP)

vom … Vorentwurf vom 25. Juli 2022

Der Schweizerische Bundesrat,

gestützt auf Artikel 48, 83 Absatz 3, 84 Absatz 1 und 86 Absatz 4 des Informationssicherheitsgesetzes vom 18. Dezember 2020[1] (ISG), Artikel 41*b* Absatz 5 des Ausländer- und Integrationsgesetzes vom 16. Dezember 2005[2] (AIG), Artikel 119 des Asylgesetzes vom 26. Juni 1998[3] (AsylG), Artikel 6*a* Absatz 5 des Ausweisgesetzes vom 22. Juni 2001[4] (AwG), Artikel 37 Absatz 1 des Bundespersonalgesetzes vom 24. März 2000[5] (BPG), Artikel 14 Absatz 2 und 150 Absatz 1 des Militärgesetzes vom 3. Februar 1995[6] (MG), Artikel 24 Absatz 4 des Kernenergiegesetzes vom 21. März 2003[7] (KEG) sowie Artikel 20*a* Absatz 2 des Stromversorgungsgesetzes vom 23. März 2007[8] (StromVG),

verordnet:

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Gegenstand

(Art. 2 Abs. 3 und 4, 28, 30, 31 und 48 ISG)

1 Diese Verordnung regelt die folgenden Verfahren:

a. die Personensicherheitsprüfungen (PSP) nach dem ISG;

b. die Sicherheitsprüfungen nach den Artikeln 41b Absatz 2 AIG und 6a Absatz 2 AwG;

c. die Prüfungen der Vertrauenswürdigkeit nach den Artikeln 29a AsylG, 20b BPG, 14 MG und 20a StromVG;

d. die Personensicherheitsprüfungen nach den Artikeln 23 Absatz 2 Buchstabe d und 103 Absatz 3 Buchstabe d MG;

SR .....

1 SR **128**
2 SR **142.20**
3 SR **142.31**
4 SR **143.1**
5 SR **172.220.1**
6 SR **510.10**
7 SR **732.1**
8 SR **734.7**

e. die Beurteilungen des Gefährdungs- oder Missbrauchpotenzials nach Artikel 113 Absatz 4 Buchstabe d MG;

f. die Zuverlässigkeitskontrollen nach Artikel 24 KEG.

2 Sie regelt zudem:

a. die Organisation der für die Durchführung der Personensicherheitsprüfungen zuständigen Fachstellen (Fachstellen PSP);

b. die Sicherheitsbescheinigung für Personen im internationalen Verhältnis;

c. die Verantwortung für den Datenschutz in Zusammenhang mit dem Informationssystem nach Artikel 45 ISG sowie die Datensicherheit;

d. die periodische Kontrolle der Bearbeitung von Personendaten im Rahmen der Personensicherheitsprüfungen durch eine externe Stelle.

3 Sie legt im Zuständigkeitsbereich des Bundesrats fest:

a. die Funktionen, welche die Ausübung einer Tätigkeit nach Absatz 1 erfordern;

b. die Zuordnung der sicherheitsempfindlichen Tätigkeiten zu den Prüfstufen;

c. die zuständigen einleitenden und entscheidenden Stellen.

Art. 2 Geltungsbereich

Diese Verordnung gilt unter Vorbehalt von Artikel 84 Absatz 3 ISG und Artikel 2 Absätze 2–5 der Informationssicherheitsverordnung vom …[9] für die verpflichteten Behörden und Organisationen nach Artikel 2 ISG.

2. Abschnitt: Funktionenlisten

Art. 3 Zuordnung
(Art. 28 Abs. 1 ISG und 24 Abs. 1 KEG)

1 Für die Bundesverwaltung gelten folgende Funktionenlisten:

a. für Personensicherheitsprüfungen nach dem ISG: die Funktionenliste nach Anhang 1;

b. für Prüfungen der Vertrauenswürdigkeit nach dem AsylG: die Funktionenliste nach Anhang 2;

c. für Prüfungen der Vertrauenswürdigkeit nach dem BPG: die Funktionenliste nach Anhang 3.

2 Für die Armee gelten folgende Funktionenlisten:

a. für Personensicherheitsprüfungen nach dem ISG: die Funktionenliste nach Anhang 4;

b. für Prüfungen der Vertrauenswürdigkeit nach Artikel 14 MG: die Funktionenliste nach Anhang 5.

9 SR **128.xxx**

3 Für Funktionen nach Artikel 20*a* Absatz 1 StromVG gilt die Funktionenliste nach Anhang 6.

4 Die Inhaber einer Bau- oder Betriebsbewilligung und die Adressaten einer Stilllegungsverfügung für Kernanlagen führen eine Liste der Funktionen, die eine Zuverlässigkeitskontrolle nach Artikel 24 Absatz 1 KEG erfordern. Das Eidgenössische Nuklearsicherheitsinspektorat (ENSI) legt die Anforderungen an diese Listen und deren Aktualisierung in Richtlinien fest.

Art. 4 Änderung

Das VBS kann auf Antrag der Departemente und der Bundeskanzlei die Funktionenlisten nach den Anhängen 1–6 ergänzen oder ändern. Es konsultiert vorgängig die Fachstelle des Bundes für Informationssicherheit.

Art. 5 Veröffentlichung, Aufbewahrung und Bekanntgabe

1 Die Anhänge 1, 4 und 6 werden nach Artikel 6 des Publikationsgesetzes vom 18. Juni 2004[10] in der Amtlichen Sammlung nicht veröffentlicht.

2 Das VBS bewahrt die Funktionenlisten nach den Anhängen 1, 4 und 6 auf und gibt sie den Stellen und Personen, welche Aufgaben nach dieser Verordnung erfüllen, bekannt.

Art. 6 Aktualitätsprüfung
(Art. 28 Abs. 2 ISG)

1 Die Departemente und die Bundeskanzlei prüfen die Aktualität der Funktionenlisten in ihrem Zuständigkeitsbereich:

a. mindestens alle vier Jahre;

b. bei Reorganisationen oder der Übernahme oder Abgabe von Aufgaben.

2 Sie erstatten dem VBS darüber Bericht und stellen bei Bedarf Antrag auf Änderung nach Artikel 4.

3. Abschnitt: Prüfungen ohne Funktionenlisten

Art. 7 Ausserordentliche Prüfung

Das VBS entscheidet im Einzelfall auf Antrag des Departements oder der Bundeskanzlei darüber, ob eine Person, die eine Funktion ausüben soll, die noch nicht in einer Funktionenliste nach den Anhängen 1–6 enthalten ist, geprüft wird. Es konsultiert vorgängig die Fachstelle des Bundes für Informationssicherheit.

10 SR **170.512**

Art. 8 Prüfungen bei kantonalen Angestellten und Dritten
(Art. 29 Abs. 1 Bst. b und c sowie 3 ISG und 24 Abs. 1 KEG)

1 Das VBS entscheidet auf Antrag des Kantons, für welche Funktionen der kantonalen Angestellten eine Personensicherheitsprüfung nach Artikel 29 Absatz 1 Buchstabe b ISG durchgeführt wird. Es konsultiert vorgängig die Fachstelle des Bundes für Informationssicherheit.

2 Ob für Dritte, die für die Bundesverwaltung einen sicherheitsempfindlichen Auftrag nach Artikel 49 ISG ausführen, eine Personensicherheitsprüfung durchgeführt wird, entscheidet:

a. im Rahmen des Betriebssicherheitsverfahrens: die Fachstelle für Betriebssicherheit;

b. in allen anderen Fällen: die oder der Informationssicherheitsbeauftragte des Departements oder der Bundeskanzlei.

Art. 9 Ausserordentliche Zuverlässigkeitskontrolle des ENSI

Das ENSI entscheidet über die Zuverlässigkeit von Personen, die nur kurzzeitig Zugang zu klassifizierten Informationen über sicherungs- oder sicherheitsrelevanten Systemen von Kernanlagen und Kernmaterialien haben. Es kann dabei auf die Zuverlässigkeitskontrolle nach Artikel 24 Absatz 1 KEG verzichten und sich stattdessen insbesondere auf Auskünfte folgender Stellen stützen:

a. eines in- oder ausländischen Unternehmens, für das die zu prüfende Person tätig war oder ist;

b. einer in- oder ausländischen Handelskammer;

c. einer ausländischen Behörde aus dem Herkunftsland der zu prüfenden Person.

4. Abschnitt: Prüfstufen

Art. 10 Personensicherheitsprüfungen nach dem ISG
(Art. 30 ISG)

1 Einer Grundsicherheitsprüfung sind folgende sicherheitsempfindliche Tätigkeiten nach dem ISG zugeordnet:

a. die Bearbeitung «vertraulich» klassifizierter Informationen;

b. die Verwaltung, der Betrieb, die Wartung oder die Überprüfung von Informatikmitteln der Sicherheitsstufe «hoher Schutz»;

c. der Zugang zu Sicherheitszonen, insbesondere zu Schutzzone 2 oder 3 einer Anlage nach der Gesetzgebung über den Schutz militärischer Anlagen;

d. Tätigkeiten, die aufgrund eines völkerrechtlichen Vertrags einer Prüfung auf dieser Prüfstufe unterzogen werden müssen.

2 Einer erweiterten Personensicherheitsprüfung sind folgende sicherheitsempfindliche Tätigkeiten nach dem ISG zugeordnet:

a. die Bearbeitung «geheim» klassifizierter Informationen;

b. die Verwaltung, der Betrieb, die Wartung oder die Überprüfung von Informatikmitteln der Sicherheitsstufe «sehr hoher Schutz»;

c. sicherheitsempfindliche Tätigkeiten von Angestellten des Bundes oder externen Mitarbeitenden:
   1. beim Nachrichtendienst des Bundes (NDB),
   2. beim militärischen Nachrichtendienst (MND),
   3. beim Zentrum elektronische Operationen der Führungsunterstützungsbasis (ZEO),
   4. bei der unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten (AB-ND);

d. sicherheitsempfindliche Tätigkeiten von Mitarbeitenden der kantonalen Vollzugsbehörden nach Artikel 9 des Nachrichtendienstgesetzes vom 25. September 2015[11] (NDG);

e. Tätigkeiten, die aufgrund eines völkerrechtlichen Vertrags einer Prüfung auf dieser Prüfstufe unterzogen werden müssen.

Art. 11 Prüfung der Vertrauenswürdigkeit nach dem BPG

[1] Einer Grundsicherheitsprüfung sind folgende Tätigkeiten nach Artikel 20*b* BPG zugeordnet:

a. hoheitliche Tätigkeiten von im Ausland eingesetzten Angestellten des Bundes und von versetzungspflichtigen Angestellten des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA);

b. Tätigkeiten nach Artikel 20*b* Absatz 1 Buchstabe b BPG, bei deren ungetreuer Ausführung ein Schaden von fünfzig Millionen bis fünfhundert Millionen Franken entstehen kann;

c. Tätigkeiten im Rahmen von Strafverfolgungs- oder polizeilichen Aufgaben:
   1. in Bezug auf die operativen Mittel und Methoden zur Bekämpfung von Verbrechen oder Vergehen,
   2. in Bezug auf die Identität exponierter Personen,
   3. von Personal des Bundesamts für Polizei (fedpol) und des Bundesamts für Justiz;

d. Tätigkeiten, die von Personen ausgeübt werden, die einer Departementsvorsteherin oder einem Departementsvorsteher oder der Bundeskanzlerin oder dem Bundeskanzler direkt unterstellt sind oder die zu ihrem oder seinem engsten Stab gehören.

[2] Einer erweiterten Personensicherheitsprüfung sind folgende Tätigkeiten nach Artikel 20*b* BPG zugeordnet:

11 SR **121**

a. Tätigkeiten von Funktionen, für die nach Artikel 2 Absatz 1 der Bundespersonalverordnung vom 3. Juli 2001[12] (BPV) der Bundesrat für die Begründung, Änderung und Beendigung des Arbeitsverhältnisses zuständig ist;

b. Tätigkeiten im Rahmen von Arbeitsverhältnissen, für deren Begründung, Änderung und Beendigung nach Artikel 2 Absatz 1bis BPV die Departementsvorsteherin oder der Departementsvorsteher oder der Bundeskanzlerin oder dem Bundeskanzler zuständig ist;

c. Tätigkeiten von Leiterinnen und Leitern von dezentralisierten Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe e BPG;

d. Tätigkeiten nach Artikel 20*b* Absatz 1 Buchstabe b BPG, bei deren ungetreuen Ausführung ein Schaden von über fünfhundert Millionen Schweizer Franken entstehen kann;

e. Tätigkeiten der Angestellten der Fachstellen PSP.

Art. 12 Prüfungen nach dem MG

1 Einer Grundsicherheitsprüfung sind folgende Tätigkeiten und Prüfungen nach dem MG zugeordnet:

a. im Ausland in Uniform ausgeübte Tätigkeiten nach Artikel 14 Absatz 1 Buchstabe a MG, die in hoheitlicher Vertretung der Schweiz oder im Bereich der militärischen Diplomatie ausgeübt werden;

b. Tätigkeiten nach Artikel 14 Absatz 1 Buchstabe b MG, bei deren ungetreuer Ausführung ein Schaden von fünfzig bis fünfhundert Millionen Franken entstehen kann;

c. Prüfungen nach Artikel 23 Absatz 2 Buchstabe d MG.

2 Eine Personensicherheitsprüfung nach Artikel 103 MG darf für Anwärterinnen und Anwärter nur verlangt werden, wenn:

a. ein Prüfgrund nach Artikel 10 oder Absatz 1 vorliegt; und

b. die Mindestfrist der Wiederholung nach Artikel 43 Absatz 1 ISG abgelaufen ist.

Art. 13 Zuverlässigkeitskontrollen nach dem KEG

1 Einer Grundsicherheitsprüfung sind die Zuverlässigkeitskontrollen nach Artikel 24 Absatz 1 KEG von folgenden Personen zugeordnet:

a. Personen, die beim Inhaber einer Bau- oder Betriebsbewilligung oder beim Adressaten einer Stilllegungsverfügung für Kernanlagen angestellt sind und Zugang zu als «vertraulich» klassifizierten Informationen über Kernanlagen und Kernmaterialien haben;

12 SR **172.220.111.3**

b. Personen, die für längere Zeit Zugang zu klassifizierten Informationen über sicherungs- oder sicherheitsrelevante Systeme von Kernanlagen und Kernmaterialien haben;

c. Personen, die im Sicherungsbereich von Kernanlagen tätig sind, insbesondere das Wachpersonal.

2 Einer erweiterten Personensicherheitsprüfung sind die Zuverlässigkeitskontrollen von Personen zugeordnet, die beim Inhaber einer Bau- oder Betriebsbewilligung oder beim Adressaten einer Stilllegungsverfügung für Kernanlagen angestellt sind und Zugang zu als «geheim» klassifizierten Informationen über Kernanlagen und Kernmaterialien haben.

Art. 14 Prüfungen der Vertrauenswürdigkeit nach dem StromVG

1 Einer Grundsicherheitsprüfung sind Tätigkeiten für die nationale Netzgesellschaft nach Artikel 18 StromVG zugeordnet, zu deren Erfüllung ein Zugang zu kritischen Informationen mit Bezug auf die Versorgungssicherheit, zu kritischen Applikationen oder kritischen Infrastrukturen benötigt wird.

2 Einer erweiterten Personensicherheitsprüfung sind Tätigkeiten für die nationale Netzgesellschaft zugeordnet, zu deren Erfüllung ein Zugang zu höchstkritischen Informationen mit Bezug auf die Versorgungssicherheit, zu höchstkritischen Applikationen oder höchstkritischen Infrastrukturen benötigt wird.

5. Abschnitt: Durchführung

Art. 15 Einleitende und entscheidende Stellen
(Art. 31 Abs. 1 ISG)

1 Die Departemente und die Bundeskanzlei legen in ihrem Zuständigkeitsbereich die einleitenden und entscheidenden Stellen fest und teilen diese den Fachstellen PSP mit.

2 Ist der Bundesrat für die Wahl oder die Übertragung des Amtes oder der Funktion zuständig, so ist er entscheidende Stelle.

3 Für Zuverlässigkeitskontrollen nach Artikel 24 Absatz 1 KEG gelten folgende Zuständigkeiten:

a. einleitende Stellen: die Inhaber von Bau- oder Betriebsbewilligungen oder die Adressaten von Stilllegungsverfügungen für Kernanlagen;

b. entscheidende Stelle: das ENSI.

4 Für Prüfungen der Vertrauenswürdigkeit nach Artikel 20*a* StromVG ist die nationale Netzgesellschaft einleitende und entscheidende Stelle.

5 Die verpflichteten Behörden und die Kantone teilen den Fachstellen PSP mit, welche Stellen in ihrem Zuständigkeitsbereich einleitende und entscheidende Stellen sind.

Art. 16 Fachstellen PSP
(Art. 31 Abs. 2 ISG)

1 Die Fachstellen PSP sind:

a. die Fachstelle PSP der Bundeskanzlei (Fachstelle PSP BK);

b. die Fachstelle PSP des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (Fachstelle PSP VBS).

2 Die Fachstelle PSP BK ist zuständig für die Prüfung von Personen, die eine der folgenden Funktionen ausüben:

a. Funktionen, bei denen der Bundesrat nach Artikel 2 Absatz 1 BPV[13] für die Begründung, Änderung und Beendigung des Arbeitsverhältnisses zuständig ist, mit Ausnahme von Funktionen innerhalb der Bundeskanzlei;

b. Funktionen im Rahmen von Arbeitsverhältnissen, für deren Begründung, Änderung und Beendigung nach Artikel 2 Absatz 1bis BPV die Departementsvorsteherin oder der Departementsvorsteher oder der Bundeskanzlerin oder dem Bundeskanzler zuständig ist;

c. Funktionen innerhalb der Fachstelle PSP VBS;

d. Funktionen innerhalb des VBS, die Führungsaufgaben gegenüber der Fachstelle PSP VBS enthalten.

3 Die Fachstelle PSP VBS ist zuständig für alle übrigen Prüfungen.

Art. 17 Überprüfung der Voraussetzungen für die Prüfung
(Art. 31 Abs. 2 ISG)

1 Nach der Einleitung einer Prüfung überprüfen die Fachstellen PSP, ob:

a. die betreffende Funktion auf der Funktionenliste enthalten ist;

b. die Prüfung von der dafür zuständigen Stelle eingeleitet wurde;

c. die zu prüfende Person in die Durchführung der Prüfung eingewilligt hat, sofern dies erforderlich ist;

d. gegebenenfalls die Zustimmung der zuständigen Stelle nach den Artikeln 7 oder 8 (Absatz 2) vorliegt.

2 Bei der ausserordentlichen Wiederholung einer Prüfung überprüfen sie, ob die Wiederholung hinreichend begründet ist.

3 Ist eine Voraussetzung nach den Absätzen 1 und 2 nicht erfüllt, so führen die Fachstellen PSP die Prüfung nicht durch und teilen dies der einleitenden Stelle unverzüglich mit.

Art. 18 Mitwirkung
(Art. 32 Abs. 3 ISG)

1 Die zu prüfenden Person muss insbesondere:

13 SR **172.220.111.3**

a. die für die Prüfung zweckmässigen Unterlagen und Daten einreichen;

b. wahrheitsgemäss Auskunft erteilen.

2 Kommt die zu prüfende Person ihrer Mitwirkungspflicht trotz entsprechender Ermahnung nicht nach, so würdigen die Fachstellen PSP dies im Rahmen der Risikobeurteilung.

3 Verweigert die zu prüfende Person die Mitwirkung, sodass keine fachgerechte Beurteilung möglich ist, so stellt die Fachstelle PSP eine Feststellungserklärung nach Artikel 39 Absatz 1 Buchstabe d ISG aus.

Art. 19 Datenerhebung
(Art. 34 ISG)

1 Die Fachstellen PSP können die Daten nach Anhang 7 erheben und bearbeiten.

2 Eine Befragung nach Artikel 34 Absatz 2 Buchstaben d ISG wird durchgeführt, wenn:

a. nach Artikel 2 Absatz 1 BPV[14] der Bundesrat für die Begründung, Änderung und Beendigung des Arbeitsverhältnisses zuständig ist;

b. nach Artikel 2 Absatz 1bis BPV die Departementsvorsteherin oder der Departementsvorsteher oder die Bundeskanzlerin oder der Bundeskanzler für die Begründung, Änderung und Beendigung des Arbeitsverhältnisses zuständig ist;

c. die zu prüfende Person bei einer der folgenden Stellen eine Funktion ausübt oder dafür vorgesehen ist:
   1. NDB,
   2. kantonale Vollzugsbehörde nach Artikel 9 NDG[15],
   3. MND,
   4. ZEO,
   5. AB-ND,
   6. fedpol,
   7. Fachstellen PSP;

d. die zu prüfende Person als Angestellte oder Angestellter des Bundes «geheim» klassifizierter Informationen bearbeiten muss und:
   1. dadurch einen weitreichenden Einblick in wichtige sicherheitspolitische Geschäfte haben und darauf wesentlich Einfluss nehmen kann, oder
   2. Aufsichts- oder Koordinationsaufgaben über Funktionen nach Buchstabe c hat;

e. aufgrund eines völkerrechtlichen Vertrags eine Befragung vorgeschrieben ist.

3 Bei der Wiederholung von Personensicherheitsprüfungen kann auf die Befragung verzichtet werden.

14 SR **172.220.111.3**
15 SR **121**

4 Eine Befragung nach Artikel 34 Absatz 3 ISG beziehungsweise Artikel 113 Absatz 5 Buchstabe e MG kann bei folgenden Dritten durchgeführt werden:

a. medizinische und psychologische Fachpersonen, die die zu prüfende Person betreuen oder betreuten;

b. Bildungsinstitutionen, an denen die zu prüfende Person Bildungen absolviert hat;

c. ehemalige und aktuelle berufliche oder militärische Vorgesetzte der zu prüfenden Person;

d. andere Personen, von denen sachdienliche Informationen zur zu prüfenden Person zu erwarten sind.

5 Die Fachstellen PSP können die Befragungen mit Hilfe von audiovisuellen Mitteln durchführen.

Art. 20 Amtshilfe
(Art. 35 ISG)

1 Die nach Artikel 34 ISG für die Erhebung von Daten im Ausland zuständigen Behörden oder Organisationen übermitteln die erhobenen Daten an die Fachstellen PSP mit:

a. Angabe der Datenquellen;

b. einer Beurteilung der Zuverlässigkeit der Daten und Datenquellen.

2 Als sicherheitsrelevant nach Artikel 35 Absatz 2 ISG gelten alle Daten, die für sich allein oder im Zusammenhang mit anderen Daten konkrete Anhaltspunkte auf Sicherheitsrisiken ergeben können.

Art. 21 Zusammenlegung von Prüfverfahren

1 Unterliegt eine Tätigkeit mehreren Prüfungen nach Artikel 1 Absatz 1, so wird nur ein Prüfverfahren durchgeführt.

2 Ist die Tätigkeit nach Absatz 1 verschiedenen Prüfstufen zugeordnet, so wird das Prüfverfahren nach den Anforderungen der höheren Prüfstufe durchgeführt; vorbehalten bleibt Artikel 27.

3 Sind sowohl die Fachstelle PSP BK als auch die Fachstelle PSP VBS für die Prüfung zuständig, so führt die Fachstelle PSP BK die Prüfung durch. Ausgenommen sind Beurteilungen des Gefährdungs- oder Missbrauchspotenzials nach Artikel 113 Absatz 4 Buchstabe d MG, die immer von der Fachstelle PSP VBS durchgeführt werden.

4 Die zuständige Fachstelle PSP hält in der Erklärung nach Artikel 39 Absatz 1 ISG das Ergebnis der Beurteilung jeder einzelnen Prüfung fest.

Art. 22 Auflagen
(Art. 39 Abs. 1 Bst. b ISG)

Die Fachstellen PSP können den entscheidenden Stellen empfehlen:

a. die geprüfte Person zu verpflichten, persönliche Daten gegenüber der entscheidenden Stelle offenzulegen, insbesondere:
   1. Daten über Beziehungen zu Dritten,
   2. Finanzdaten, einschliesslich Daten betreffend Bankkonten und Steuern,
   3. Daten über Abklärungen nach Buchstabe b,
   4. Daten über im Zeitpunkt der Erklärung hängige Verfahren;

b. medizinische oder psychologische Abklärungen durchführen zu lassen, insbesondere Abklärungen betreffend die Urteils- und Entscheidfähigkeit der zu prüfenden Person sowie den Konsum von Drogen und Betäubungsmitteln;

c. Massnahmen nach Artikel 25 BPG zu treffen;

d. Massnahmen betreffend den Besitz der persönlichen Waffe zu ergreifen, sofern es sich bei der zu prüfenden Person um eine Angehörige oder einen Angehörigen der Armee handelt;

e. andere Massnahmen zu treffen, die im Einzelfall geeignet erscheinen, das festgestellte Sicherheitsrisiko auf ein tragbares Mass zu reduzieren.

Art. 23 Mitteilung
(Art. 40 ISG)

[1] Untersteht eine Person nacheinander verschiedenen Prüfgründen und stellt eine Fachstelle PSP bei der späteren Prüfung ein Sicherheitsrisiko fest, so teilt sie ihre Erklärung den für die früheren Prüfungen entscheidenden Stellen mit.

[2] Die Fachstellen PSP teilen vorläufige Erkenntnisse mit, wenn Anzeichen für ein Sicherheitsrisiko bestehen, das dringenden Handlungsbedarf erfordert. Bei Prüfungen von Stellungspflichtigen oder Angehörigen der Armee können dies insbesondere sein:

a. Strafurteile;

b. laufende polizeiliche Ermittlungen, Strafuntersuchungen oder Strafverfahren wegen eines Verdachts auf ein begangenes Vergehen oder Verbrechen; die Mitteilung darf nur erfolgen, wenn das laufende Verfahren nach Beurteilung der ermittlungs- oder verfahrensleitenden Stelle dadurch nicht gefährdet ist;

c. ernstzunehmende Anzeichen oder Hinweise nach Artikel 113 Absatz 1 MG oder ein Verdacht auf solche Anzeichen oder Hinweise;

d. Anzeichen oder Hinweise auf eine eingeschränkte Militärdiensttauglichkeit, Militärdienstuntauglichkeit oder eine Funktionsunfähigkeit;

e. ernstzunehmende Anzeichen oder Hinweise, dass sie sich selbst oder Dritte gefährden könnten.

[3] Die entscheidenden Stellen teilen den Fachstellen PSP mit, an welche Person oder Stelle die Mitteilungen nach den Absätzen 1 und 2 erfolgen sollen.

6. Abschnitt: Folgen der Erklärung

Art. 24 Ausübung der Tätigkeit
(Art. 41 ISG)

1 Die entscheidende Stelle lässt die geprüfte Person die Tätigkeit nur dann ausüben, wenn sie die erkannten Risiken als tragbar beurteilt oder mit Auflagen nach Artikel 22 auf ein tragbares Mass reduzieren kann.

2 Bei Erklärungen nach Artikel 39 Absatz 1 Buchstaben b–d ISG teilt sie ihren Entscheid der geprüften Person und der zuständigen Fachstelle PSP innerhalb von einem Monat mit. Bei einer Sicherheitserklärung nach Artikel 39 Absatz 1 Buchstabe a ISG wird die Zulassung zur Ausübung der Tätigkeit vermutet.

Art. 25 Mehrmalige Verwendung einer Erklärung
(Art. 42 ISG)

1 Liegt für eine Person eine gültige Erklärung aufgrund einer früheren Prüfung vor, so kann die entscheidende Stelle auf eine neue Beurteilung verzichten, wenn:

a. der früheren Beurteilung dieselben Risikofaktoren zugrunde lagen wie der neuen Prüfung; und

b. kein Grund für eine ausserordentliche Wiederholung besteht.

2 Sicherheitsrisiken, die bei einer Beurteilung auf einer höheren Prüfstufe festgestellt wurden, dürfen nur berücksichtigt werden, wenn:

a. diese Risiken auch aufgrund der Daten, die auf einer niedrigeren Prüfstufe erhoben werden, erkannt werden könnten; oder

b. das öffentliche Interesse nach Artikel 1 Absatz 2 ISG gegenüber dem Persönlichkeitsrecht der geprüften Person überwiegt.

Art. 26 Ordentliche Wiederholung
(Art. 43 Abs. 1 und 2 ISG)

1 Eine ordentliche Wiederholung einer Prüfung ist einzuleiten:

a. innerhalb von drei Monaten vor Ablauf der Maximalfrist nach Artikel 43 Absatz 1 ISG: wenn bei der vorangegangenen Prüfung eine Sicherheitserklärung nach Artikel 39 Absatz 1 Buchstabe a ISG ausgestellt wurde;

b. innerhalb von drei Monaten nach Ablauf der Mindestfrist nach Artikel 43 Absatz 1 ISG: wenn bei der vorangegangenen Prüfung eine Erklärung nach Artikel 39 Absatz 1 Buchstaben b–d ISG ausgestellt;

c. für Funktionen der Armee und des Zivilschutzes, für deren Ausübung eine Grundsicherheitsprüfung notwendig ist: wenn die zu prüfende Person die Funktion voraussichtlich noch mindestens fünf Jahre ausüben soll.

2 Vorbehalten bleiben Fristen aufgrund eines völkerrechtlichen Vertrags.

Art. 27 Ausserordentliche Wiederholung
(Art. 43 Abs. 3 ISG)

1 Hat die entscheidende Stelle Grund anzunehmen, dass seit der letzten Prüfung wesentliche Risiken entstanden sind, die ohne erneute Prüfung nicht beurteilt werden können, so leitet sie sofort eine ausserordentliche Wiederholung der Prüfung ein.

2 Hat sie Grund anzunehmen, dass bei der letzten Prüfung festgestellte Risiken weggefallen sind, so kann sie eine ausserordentliche Wiederholung der Prüfung einleiten.

Art. 28 Wirkung der Wiederholung
(Art. 43 ISG)

1 Die betroffene Person gilt bis zum neuen Entscheid nach Artikel 24 Absatz 2 als nach dem bisherigen Entscheid geprüft.

2 Ergeben sich vor der Eröffnung des neuen Entscheids Anzeichen, dass neue Sicherheitsrisiken bestehen, so trifft die entscheidende Stelle die notwendigen vorsorglichen Massnahmen.

Art. 29 Rechtsschutz
(Art. 44 Abs. 3 ISG)

Die Fachstellen PSP sind betreffend Entscheide des Bundesverwaltungsgerichts zu ihren Erklärungen zur Beschwerde an das Bundesgericht berechtigt.

Art. 30 Sicherheitsbescheinigung im internationalen Verhältnis
(Art. 48 Bst. c ISG)

1 Für die Ausstellung von Sicherheitsbescheinigungen im internationalen Verhältnis ist die Fachstelle des Bundes für Informationssicherheit zuständig.

2 Eine Sicherheitsbescheinigung wird auf Antrag ausgestellt, wenn:

a. eine Prüfung auf der erforderlichen Prüfstufe durchgeführt wurde;

b. die betreffende Person zur Ausübung der Tätigkeit zugelassen wurde; und

c. die betreffende Person nachweisbar zur Ausübung der Tätigkeit ausgebildet wurde.

3 Gehört die beantragende Stelle nicht zur Bundesverwaltung und benötigt sie die Sicherheitsbescheinigung nicht für einen Auftrag des Bundes, so trägt sie die Kosten des Verfahrens.

7. Abschnitt: Bearbeitung von Personendaten

Art. 31 Verantwortung für den Datenschutz und die Datensicherheit
(Art. 48 Bst. d ISG)

1 Die Fachstelle PSP VBS ist für den Schutz und die Sicherheit des Informationssystems nach Artikel 45 ISG sowie der darin enthaltenen Daten verantwortlich.

2 Für den Schutz und die Sicherheit von Daten, die ausserhalb des Informationssystems nach Artikel 45 Absatz 5 ISG bearbeitet werden, ist die bearbeitende Stelle verantwortlich.

Art. 32 Periodische Kontrolle der Bearbeitung von Personendaten
(Art. 48 Bst. e ISG)

Das VBS und die Bundeskanzlei sorgen dafür, dass eine unabhängige Stelle mindestens alle fünf Jahre die rechtmässige Bearbeitung der Personendaten durch ihre Fachstellen PSP prüft.

8. Abschnitt: Schlussbestimmungen

Art. 33 Elektronischer Geschäftsverkehr
(Art. 48 Bst. a ISG)

Das VBS regelt nach Konsultation der Bundeskanzlei den elektronischen Geschäftsverkehr.

Art. 34 Gebührenerhebung

1 Für die Durchführung von Prüfungen bei Stellen ausserhalb der zentralen Bundesverwaltung erheben die Fachstellen PSP Gebühren nach Zeitaufwand.

2 Es gilt ein Stundenansatz von 100–400 Franken. Dieser richtet sich insbesondere nach der Dringlichkeit des Geschäfts und der Funktionsstufe des ausführenden Personals.

3 Im Übrigen gilt die Allgemeine Gebührenverordnung vom 8. September 2004[16] (AllgGebV).

Art. 35 Leistungen der Fachstellen PSP zugunsten der Kantone
(Art. 86 Abs. 4 ISG)

1 Die Kantone können Leistungen der Fachstelle PSP VBS für ihre eigene Informationssicherheit in Anspruch nehmen, wenn sie:

a. über eine ausreichende gesetzliche Grundlage für Prüfungen nach dieser Verordnung verfügen;

b. zur Gewährleistung der Informationssicherheit ähnliche Beurteilungen wie der Bund vornehmen wollen; und

c. mit dem VBS eine Leistungsvereinbarung abgeschlossen haben.

2 Das VBS regelt in den Leistungsvereinbarungen nach Absatz 1 Buchstabe c insbesondere:

a. die Anzahl durchzuführender Prüfungen;

16 SR **172.041.1**

b. die einleitenden und entscheidenden Stellen bei den Kantonen;

c. die Finanzierung der Leistungen, einschliesslich die Modalitäten.

3 Die Höhe der Gebühren bemisst sich nach dem Zeitaufwand. Es gilt ein Stundenansatz von 100–400 Franken. Dieser richtet sich namentlich nach der Dringlichkeit des Geschäfts und der Funktionsstufe des ausführenden Personals. Im Übrigen gilt die AllgGebV[17].

Art. 36 Aufhebung anderer Erlasse

Die folgenden Erlasse werden aufgehoben:

a. die Verordnung vom 4. März 2011[18] über die Personensicherheitsprüfungen;

b. die Verordnung der Bundeskanzlei vom 30. November 2011[19] über die Personensicherheitsprüfungen;

c. die Verordnung des WBF vom 2. November 2011[20] über die Personensicherheitsprüfungen;

d. die Verordnung des VBS vom 12. März 2012[21] über die Personensicherheitsprüfungen;

e. die Verordnung des EDA vom 14. August 2012[22] über die Personensicherheitsprüfungen;

f. die Verordnung des UVEK vom 15. Februar 2013[23] über die Personensicherheitsprüfungen;

g. die Verordnung des EJPD vom 26. Juni 2013[24] über die Personensicherheitsprüfungen;

h. die Verordnung des EDI vom 12. August 2013[25] über die Personensicherheitsprüfungen;

i. die Verordnung vom 9. Juni 2006[26] über die Personensicherheitsprüfungen im Bereich Kernanlagen.

Art. 37 Änderung anderer Erlasse

Die Änderung anderer Erlasse wird in Anhang 8 geregelt.

17 SR **172.041.1**
18 [AS **2011** 5903, **2012** 1153 3631 3765 5527 6669, **2013** 3041, **2014** 4567, **2016** 1785, **2017** 4151 4231, **2020** 5893]
19 [AS **2011** 6077, **2016** 1365]
20 [AS **2011** 4999, **2013** 1335]
21 [AS **2012** 1161 1597]
22 [AS **2012** 4241]
23 [AS **2013** 765]
24 [AS **2013** 2633]
25 [AS **2013** 2675]
26 [AS **2006** 2481, **2008** 547, **2011** 1031]

Art. 38 Übergangsbestimmungen

[1] Im Zeitpunkt des Inkrafttretens dieser Verordnung hängige Beurteilungen werden nach dem ISG und dieser Verordnung weitergeführt oder eingestellt.

[2] Nach bisherigem Recht durchgeführte Personensicherheitsprüfungen entsprechen während der Übergangsfrist nach Artikel 90 Absatz 3 ISG wie folgt den Prüfstufen nach neuem Recht:

a. Grundsicherheitsprüfung nach bisherigem Recht: Grundsicherheitsprüfung nach neuem Recht;

b. erweiterte Personensicherheitsprüfung nach bisherigem Recht: erweiterte Personensicherheitsprüfung nach neuem Recht;

c. erweiterte Personensicherheitsprüfung mit Befragung nach bisherigem Recht: erweiterte Personensicherheitsprüfung nach neuem Recht.

[3] Personen in Funktionen, für die nach neuem Recht eine Prüfung oder eine Prüfung in einer höheren Prüfstufe durchgeführt werden muss, gelten bis zum Entscheid nach Artikel 24 Absatz 2 als geprüft, wenn die neu erforderliche Prüfung innerhalb von drei Monaten nach Inkrafttreten dieser Verordnung eingeleitet wird. Ergeben sich während der Prüfung Anzeichen auf Sicherheitsrisiken, so trifft die entscheidende Stelle die notwendigen vorsorglichen Massnahmen.

[4] Sicherheitsprüfungen, die die nationale Netzgesellschaft vor Inkrafttreten dieser Verordnung und vor Ablauf der Frist nach Absatz 5 auf privatrechtlicher Basis erhalten hat, bleiben im Rahmen der Wiederholungsfristen nach den Artikeln 26 und 27 wie folgt verwendbar:

a. Sicherheitsprüfungen für kritische Funktionen: als Grundsicherheitsprüfung nach dieser Verordnung;

b. Sicherheitsprüfungen für höchst kritische Funktionen: als erweiterte Personensicherheitsprüfung nach dieser Verordnung.

[5] Die nationale Netzgesellschaft ist berechtigt, bis ein Jahr nach Inkrafttreten dieser Verordnung Prüfungen der Vertrauenswürdigkeit nach Artikel 20*a* StromVG auf privatrechtlicher Basis durchführen zu lassen.

Art. 39 Inkrafttreten

Diese Verordnung tritt am … 2023 in Kraft:

… Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Ignazio Cassis
Der Bundeskanzler: Walter Thurnherr

Anhang 1[27]
(Art. 3 Abs. 1 Bst. a)

Funktionen der Bundesverwaltung, die einer Personensicherheitsprüfung nach ISG unterstehen

1. in der Prüfstufe Grundsicherheitsprüfung:

Verwaltungseinheit	Funktion	Prüfgrund nach Art. 10 Abs. 1		
		Bst. a	Bst. b	Bst. c

2. in der Prüfstufe erweiterte Personensicherheitsprüfung:

Verwaltungseinheit	Funktion	Prüfgrund nach Art. 10 Abs. 2			
		Bst. a	Bst. b	Bst. c	Bst. d

27 In der AS nach Art. 6 des Publikationsgesetzes vom 18. Juni 2004 (SR **170.512**) nicht veröffentlicht.

Anhang 2
(Art. 3 Abs. 1 Bst. b)

Funktionen der Bundesverwaltung, die einer Prüfung der Vertrauenswürdigkeit nach dem AsylG unterstehen

a. …,

b. …;

c. ….

Anhang 3
(Art. 3 Abs. 1 Bst. c)

Funktionen der Bundesverwaltung, die einer Prüfung der Vertrauenswürdigkeit nach dem BPG unterstehen

1. in der Prüfstufe Grundsicherheitsprüfung:

Verwaltungseinheit	Funktion	Prüfgrund nach Art. 11 Abs. 1			
		Bst. a	Bst. b	Bst. c	Bst. d

2. in der Prüfstufe erweiterte Personensicherheitsprüfung:

Verwaltungseinheit	Funktion	Prüfgrund nach Art. 11 Abs. 2				
		Bst. a	Bst. b	Bst. c	Bst. d	Bst. e

Anhang 4[28]
(Art. 3 Abs. 2 Bst. a)

Funktionen der Armee, die einer Personensicherheitsprüfung nach dem ISG unterstehen

1. in der Prüfstufe Grundsicherheitsprüfung:

Gliederungs- und Strukturebene	Funktion	Prüfgrund nach Art. 10 Abs. 1		
		Bst. a	Bst. b	Bst. c

2. in der Prüfstufe erweiterte Personensicherheitsprüfung:

Gliederungs- und Strukturebene	Funktion	Prüfgrund nach Art. 10 Abs. 2	
		Bst. a	Bst. b

28 In der AS nach Art. 6 des Publikationsgesetzes vom 18. Juni 2004 (SR **170.512**) nicht veröffentlicht.

Anhang 5
(Art. 3 Abs. 2 Bst. b)

Funktionen der Armee, die einer Prüfung der Vertrauenswürdigkeit nach Artikel 14 MG unterstehen

in der Prüfstufe Grundsicherheitsprüfung:

Gliederungs- und Strukturebene	Funktion	Prüfgrund nach Art. 12 Abs. 1 Buchstabe a und b	
		Bst. a	Bst. b

Anhang 6[29]
(Art. 3 Abs. 3)

Funktionen nach Artikel 20*a* Absatz 1 StromVG

1. in der Prüfstufe Grundsicherheitsprüfung:

Funktion	Kritische Information / Applikation / Infrastruktur

2. in der Prüfstufe erweiterte Personensicherheitsprüfung:

Funktion	höchstkritische Information / Applikation / Infrastruktur

29 In der AS nach Art. 6 des Publikationsgesetzes vom 18. Juni 2004 (SR **170.512**) nicht veröffentlicht.

Anhang 7
(Art. 19 Abs. 1)

Datenerhebung und -bearbeitung

1. Daten, die bei allen Prüfstufen bearbeitet werden können:

a. Daten über die Identität der zu prüfenden Person, insbesondere:
   1. Name, Ledigname und Vornamen
   2. Spitzname, Aliasse, Pseudoname und Benutzername
   3. Adressen
   4. Geburtsdatum
   5. Geschlecht oder Gender
   6. Telefonnummern (Festnetz und Mobilnetz)
   7. E-Mail-Adressen (beruflich und privat)
   8. AHV-Nummer
   9. Nationalitäten
   10. Bei einer Nationalität anders als CH:
      – Datum der Einbürgerung
      – Dauer des Aufenthaltes in der Schweiz
   11. Heimatort
   12. Geburtsort
   13. frühere Wohnorte

b. Daten über die Lebensführung der zu prüfenden Person, insbesondere:
   1. beruflicher Werdegang
   2. schulischer Werdegang
   3. Werdegang innerhalb der Armee, des Zivilschutzes oder des Zivildienstes
   4. Ausbildungen
   5. Hobbies
   6. Projekte
   7. Angehörigkeit zu Vereinen
   8. ehrenamtliche Tätigkeiten
   9. religiöse Ansichten oder Tätigkeiten
   10. weltanschauliche Ansichten
   11. politische Ansichten oder Tätigkeiten
   12. gewerkschaftliche Ansichten oder Tätigkeiten

c. Daten über enge persönliche Beziehungen und familiäre Verhältnisse der zu prüfenden Person, insbesondere:
   1. Zivilstand

2. Intimsphäre und Sexualität
3. Verhältnis zur Familie
4. Identität der Eltern
5. Freundeskreis

d. Daten über die Beziehung zum Ausland der zu prüfenden Person, insbesondere:
1. Ferien
2. Sprachaufenthalte
3. Geschäftsreisen
4. personelle Beziehungen im Ausland und internationale Kontakte
5. finanzielle Interessen im Ausland

e. Daten über die Gesundheit der zu prüfenden Person, insbesondere:
1. physische und psychische Krankheiten
2. physische und psychische Behinderungen
3. Konsum von Betäubungsmittel und Alkohol
4. Süchte und Abhängigkeiten

f. Finanzdaten der zu prüfenden Person, insbesondere:
1. Bankauszüge
2. Finanzanlagen
3. Löhne
4. Hypotheken
5. Kredite
6. Vermögen
7. Steuern
8. Schulden
9. Investitionen

g. Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen, insbesondere:
1. Betreibungen und Konkurse
2. Strafuntersuchungen
3. administrative Untersuchungen
4. Klagen und rechtliche Prozesse
5. Mediation
6. Ausweisentzüge

h. Angaben über bisherige Risikofaktoren im Rahmen einer sicherheitsempfindlichen Tätigkeit

i. Daten über Dritte, insbesondere:
   1. Angaben nach den Buchstaben a–g über den (Ehe)Partnerin oder die (Ehe)Partner bzw. den Familienkreis bzw. den engen Freundeskreis, sofern diese Angaben nach Artikel 34 Absatz 3 ISG für die Beurteilung des Sicherheitsrisikos unerlässlich sind.
   2. Auftraggeber oder Auftraggeberin und dessen oder deren Adresse
   3. Projekt

j. Daten, aus Systemen und öffentlich zugänglichen Quellen, insbesondere:
   1. aus dem Strafregister: sämtliche Daten
   2. von den zivilen und militärischen Strafbehörden: sämtliche Daten
   3. von Organen des Bundes nach Artikel 34 Absatz 1 Buchstabe c ISG:
      - Daten der Waffeninformationsplattform ARMADA
      - Daten des Informationssystems HOOGAN
      - Daten des Informationssystems JANUS
      - Daten des nationalen Polizeiindex
      - Daten des automatisierten Polizeifahndungssystems RIPOL
      - Daten der Informationssysteme des NDB und des MND
      - Daten des IVZ-Registers
      - Daten des JORASYS
      - Daten der Informationssysteme des BAZG
      - Daten des zentralen Versichertenregisters der Sozialversicherungen des Bundes
      - Daten des PISA
      - Daten der Rekrutierung der Stellungspflichtigen
      - Daten zur Beurteilung der Diensttauglichkeit und Dienstfähigkeit der Stellungs-, Militärdienst- und Schutzdienstpflichtigen sowie von Zivilpersonen, die für einen befristeten Einsatz der Armee beigezogen werden
      - Daten der Armee und der Militärverwaltung über Stellungspflichtige und Angehörige der Armee

   4. aus den Registern und Akten der Sicherheitsorgane der Kantone sowie der Polizei: sämtliche Daten
   5. aus den Registern der Betreibungs- und Konkursbehörden: sämtliche Daten

6. aus den Akten bisheriger Prüfungen: sämtliche Daten, die nicht älter als zehn Jahre sind und nach Artikel 47 ISG noch nicht archiviert oder vernichtet sind.
7. aus öffentlich zugänglichen Quellen:
   - Im Internet: Daten, die jedem Internet-Benutzer oder jeder Internet-Benutzerin nach der Errichtung eines Kontos, dem Bezahlen einer Gebühr oder dem Abschluss eines Abonnements zugänglich sind.
   - In sozialen Medien: Daten, die jedem Benutzer oder jeder Benutzerin ohne persönliche Kontaktaufnahme zu einem anderen Benutzer oder einer anderen Benutzerin zugänglich sind.

2. Daten, die bei der Prüfstufe erweiterte Personensicherheitsprüfung bearbeitet werden können:

a. von eidgenössischen und kantonalen Steuerbehörden: sämtliche Daten

b. aus den Registern der Einwohnerkontrollen: sämtliche Daten

c. von Finanzinstituten und Banken nach Artikel 34 Absatz 2 Buchstabe c ISG: sämtliche Daten

d. durch Befragung der zu prüfenden Person: sämtliche Daten, die aus der übrigen Datenerhebung nicht oder nur unklar hervorgehen

Anhang 8
(Art. 37)

Änderung anderer Erlasse

Die nachstehenden Erlasse werden wie folgt geändert:

1. Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport vom 7. März 2003[30]

Art. 6 Bst. c

Aufgehoben

2. Bundespersonalverordnung vom 3. Juli 2001[31]

Art. 94e Auszug aus dem Strafregister und dem Betreibungsregister
(Art. 20*a* BPG)

[1] Der Arbeitgeber kann von Bewerberinnen, Bewerbern und Angestellten einen Auszug aus dem Strafregister und dem Betreibungsregister verlangen, wenn dies aus Gründen der Korruptionsprävention oder der Sicherheit geeignet und erforderlich ist oder wenn wirtschaftliche oder politische Interessen des Arbeitgebers gefährdet sein könnten.

[2] Der Auszug kann alle fünf Jahre oder aus wichtigen Gründen jederzeit verlangt werden.

[3] Die Kosten für die Auszüge trägt der Arbeitgeber.

Art. 94f Prüfung der Vertrauenswürdigkeit
(Art. 20*b* BPG)

[1] Eine Prüfung der Vertrauenswürdigkeit von Bewerberinnen, Bewerbern und Angestellten kann unter den Voraussetzungen der Artikel 11der Verordnung vom …[32] über die Personensicherheitsprüfungen (VPSP) durchgeführt werden.

[2] Die Funktionenliste, die Prüfstufen und das Verfahren der Prüfung sind in der VPSP geregelt.

30 SR **172.214.1**
31 SR **172.220.111.3**
32 SR …

3. Verordnung vom 24. Juni 2009[33] über internationale militärische Kontakte

Art. 5 Abs. 1 Bst. b

[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 richtet sich nach den entsprechenden Informationsschutzvorschriften, insbesondere:

b. der Verordnung vom …[34] über die Personensicherheitsprüfungen;

4. Verordnung vom 16. Dezember 2009[35] über die militärischen Informationssysteme

Art. 67 und Anh. 30

Aufgehoben

Art. 70n Bst. e

Die Daten des FABIS werden beschafft:

e. aus dem Informationssystem zur Personensicherheitsprüfung nach Artikel 45 Absatz 1 des Informationssicherheitsgesetzes vom 18. Dezember 2020[36]: die Daten nach Anhang 33*c* Ziffer 2.

Anh. 23a Ziff. 36

36. Prüfstufe nach Artikel 5 oder 6 der Verordnung vom …[37] über die Personensicherheitsprüfungen (VPSP), Datum der Rechtskraft des Entscheids nach Artikel 24 VPSP sowie Zeitpunkt der nächsten ordentlichen Wiederholung der Personensicherheitsprüfung nach Artikel 26 VPSP

Anh. 33c Ziff. 2

2. Prüfstufe nach den Artikeln 10–14 VPSP[38], Datum der Rechtskraft des Entscheids nach Artikel 24VPSP sowie Zeitpunkt der nächsten ordentlichen Wiederholung der Personensicherheitsprüfung nach Artikel 26 VPSP betreffend einer zugangsberechtigten Person.

33 SR **510.215**
34 SR **…**
35 SR **510.911**
36 SR **128**
37 SR **…**
38 SR **…**

Anh. 33d Ziff. 2

2. Prüfstufe nach den Artikeln 10–14 VPSP[39], Datum der Rechtskraft des Entscheids nach Artikel 24VPSP sowie Zeitpunkt der nächsten ordentlichen Wiederholung der Personensicherheitsprüfung nach Artikel 26 VPSP betreffend einer zugangsberechtigten Person.

5. Verordnung vom 22. November 2017[40] über die Militärdienstpflicht

Art. 11 Abs. 3 Bst. g

4 An der Orientierungsveranstaltung werden die Teilnehmenden insbesondere informiert über:

g. die Personensicherheitsprüfung nach der Verordnung vom …[41] über die Personensicherheitsprüfungen (VPSP) und die Folgen beim Vorliegen von besonderen persönlichen Verhältnissen nach Artikel 33 Absatz 2.

Art. 16 Abs. 3 Bst. b

3 Eine militärdiensttaugliche Person wird provisorisch auf eine Rekrutierungsfunktion der Armee zugeteilt, wenn:

b. eine Personensicherheitsprüfung erforderlich ist, aber noch kein Entscheid nach Artikel 24 VPSP[42] oder noch keine Information nach Artikel 23 Absatz 2 PSPV vorliegt.

Art. 21 Abs. 1 Bst. b Ziff. 3

1 Auf gemeinsames Gesuch der betroffenen Person und des zuständigen Kommandos können Spezialisten und Spezialistinnen, höhere Unteroffiziere und Stabsoffiziere für die Verlängerung der Militärdienstpflicht zugelassen werden, wenn:

b. die betroffene Person die folgenden Voraussetzungen erfüllt:

3. Die entscheidende Stelle nach Artikel 24 VPSP[43] lässt die betroffene Person die Tätigkeit ausüben.

Art. 72 Abs. 2 Bst. c

2 Für eine Einteilung in eine bestimmte Funktion oder eine Beförderung in einen höheren Grad müssen die folgenden Voraussetzungen erfüllt sein:

c. Die entscheidende Stelle nach Artikel 24 VPSP[44] lässt die betroffene Person die Tätigkeit ausüben.

39 SR **…**
40 SR **512.21**
41 SR **…**
42 SR **…**
43 SR **…**
44 SR **…**

Art. 80 Abs. 2 Bst. c

2 Zum Fachoffizier oder zur Fachoffizierin ernannt werden können Soldaten, Gefreite, Unteroffiziere und höhere Unteroffiziere, wenn:

c. die entscheidende Stelle nach Artikel 24 VPSP[45] die betroffene Person die Tätigkeit ausüben lässt.

6. Kernenergieverordnung vom 10. Dezember 2004[46]

Art. 33a Zuverlässigkeitskontrollen

1 Die periodischen Zuverlässigkeitskontrollen von Personen, die Funktionen ausüben, die für die nukleare Sicherheit und die Sicherung der Kernanlage wesentlich sind, sind in der Verordnung vom …[47] über die Personensicherheitsprüfung geregelt.

2 Die Kosten für die Prüfung trägt der Bewilligungsinhaber der Kernanlage.

45 SR **…**
46 SR **732.11**
47 SR …

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verordnung über das Betriebssicherheitsverfahren (VBSV)

vom … Vorentwurf vom 25. Juli 2022

Der Schweizerische Bundesrat,

gestützt auf die Artikel 73 und 84 Absatz 1 des Informationssicherheitsgesetzes vom 18. Dezember 2020[1] (ISG),

verordnet:

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Gegenstand und Geltungsbereich
(Art. 2, 49 und 73 ISG)

[1] Diese Verordnung regelt:

a. das Betriebssicherheitsverfahren nach den Artikeln 49–73 ISG;

b. die Anwendung des Betriebssicherheitsverfahrens auf Subunternehmen;

c. die Organisation der Fachstelle Betriebssicherheit (Fachstelle BS);

d. die Datensicherheit im Informationssystem nach Artikel 70 ISG;

e. die periodische Kontrolle der Bearbeitung von Personendaten durch eine externe Stelle.

[2] Sie gilt unter Vorbehalt von Artikel 84 Absatz 3 ISG und Artikel 2 Absätze 2–5 der Informationssicherheitsverordnung vom …[2] (ISV) für die verpflichteten Behörden und Organisationen nach Artikel 2 ISG.

Art. 2 Betroffene Betriebe
(Art. 50 ISG)

[1] Diese Verordnung ist anwendbar auf Betriebe mit Sitz in der Schweiz.

[2] Für Betriebe mit Sitz im Ausland richtet sich das Verfahren nach dem entsprechenden völkerrechtlichen Vertrag nach Artikel 87 ISG.

SR .....
1 SR **128**
2 SR **…**

Art. 3 Zuständige Behörde
(Art. 51 Abs. 2 ISG)

[1] Das [zuständige Departement] betreibt die Fachstelle BS

[2] Die Fachstelle koordiniert internationale Tätigkeiten mit der Fachstelle des Bundes für Informationssicherheit nach Artikel 83 ISG.

2. Abschnitt: Einleitung des Betriebssicherheitsverfahrens

Art. 4 Antrag auf Einleitung des Verfahrens
(Art. 52 ISG)

[1] Folgende Stellen im Zuständigkeitsbereich des Bundesrats sind für den Antrag auf Einleitung des Verfahrens an die Fachstelle BS zuständig:

a. die Informationssicherheitsbeauftragten der Verwaltungseinheiten nach Artikel 37 ISV;

b. die Betriebssicherheitsbeauftragten in Anwendung von Artikel 12 Buchstabe c.

[2] Die verpflichteten Behörden nach Artikel 2 Absatz 1 ISG melden der Fachstelle BS, wer in ihrem Zuständigkeitsbereich für den Antrag auf Einleitung des Verfahrens zuständig ist.

[3] Der Antrag umfasst insbesondere:

a. eine Umschreibung der Bauleistung, Lieferung oder Dienstleistung;

b. Erläuterungen zur Sicherheitsempfindlichkeit des Auftrags;

c. Angaben zum geplanten Vergabeverfahren.

Art. 5 Prüfung des Antrags
(Art. 53 ISG)

[1] Die Fachstelle BS nimmt vor der Einleitung des Verfahrens Rücksprache mit der Auftraggeberin oder der zuständigen ausländischen Behörde oder internationalen Organisation.

[2] Sie leitet das Verfahren auf jeden Fall ein, wenn eine der folgenden Voraussetzungen erfüllt ist:

a. Der sicherheitsempfindliche Auftrag umfasst die Bearbeitung «geheim» klassifizierter Informationen oder die Verwaltung, den Betrieb, die Wartung oder die Überprüfung von Informatikmitteln der Sicherheitsstufe «sehr hoher Schutz».

b. Der sicherheitsempfindliche Auftrag umfasst die Bearbeitung «vertraulich» klassifizierter Informationen, die mehrere Behörden oder Departemente betreffen.

c. Der sicherheitsempfindliche Auftrag umfasst die Verwaltung, den Betrieb, die Wartung oder die Überprüfung von Informatikmitteln der Sicherheitsstufe

«hoher Schutz», die für die Erfüllung behörden- oder departementsübergreifender Aufgaben eingesetzt werden.

d. Der Betrieb bewirbt sich um einen Auftrag, für den er eine internationale Betriebssicherheitsbescheinigung nach Artikel 66 ISG benötigt.

3 Die Fachstelle BS orientiert die Auftraggeberin, wenn absehbar wird, dass die Prüfung des Antrags länger als 30 Tage dauern wird.

Art. 6 Prüfung des Antrags mit ausländischen Sicherheitsbehörden
(Art. 52 Abs. 3 ISG)

1 Wenn ausländische Betriebe für die Erfüllung des sicherheitsempfindlichen Auftrags in Frage kommen, so leitet die Fachstelle BS den Antrag an die Fachstelle des Bundes für Informationssicherheit weiter.

2 Die Fachstelle des Bundes für Informationssicherheit prüft mit der zuständigen ausländischen Sicherheitsbehörde, ob die betroffenen Betriebe über eine gültige Betriebssicherheitserklärung verfügen. Ist dies nicht der Fall, so beantragen sie die Einleitung des Betriebssicherheitsverfahrens.

Art. 7 Festlegung der Sicherheitsanforderungen
(Art. 54 ISG)

1 Die Anforderungen an die Informationssicherheit während des Vergabeverfahrens und der Auftragserfüllung richten sich nach den Bestimmungen der ISV[3] und der Verordnung vom …[4] über die Personensicherheitsprüfung.

2 Wird das Verfahren auf Antrag einer ausländischen Behörde oder internationalen Organisation eingeleitet, so richten sich die Anforderungen an die Informationssicherheit nach dem entsprechenden völkerrechtlichen Vertrag.

3 Die Fachstelle BS legt in Absprache mit der Auftraggeberin fest, welche sicherheitsempfindlichen Aufgaben während des Vergabeverfahrens und der Auftragserfüllung durch die Auftraggeberin umzusetzen sind.

4 Die Auftraggeberin bleibt für die Koordination der Verfahrensabläufe im Vergabeverfahren verantwortlich.

3. Abschnitt: Beurteilung der Betriebe

Art. 8 Meldung geeigneter Betriebe
(Art. 55 ISG)

1 Die Auftraggeberin kann der Fachstelle BS bis zu fünf in Frage kommende Betriebe melden. Die Fachstelle BS kann in begründeten Ausnahmefällen auf Antrag der Auftraggeberin eine höhere Zahl zulassen.

3 SR …
4 SR …

2 Die Fachstelle BS prüft, ob die in Frage kommenden Betriebe in die Durchführung des Verfahrens eingewilligt haben.

3 Sie informiert die Auftraggeberin, wenn absehbar ist, dass die Eignungsprüfung länger als 30 Tage dauern wird.

Art. 9 Datenerhebung
(Art. 56 ISG)

1 Die Fachstelle BS erhebt sämtliche sicherheitsrelevanten Daten, die für die Beurteilung der Eignung des Betriebs notwendig sind, insbesondere:

a. Daten über die Eigentumsverhältnisse sowie geplante Änderungen wie Fusionen, Beteiligungen, Übernahmen;

b. Daten über die Zusammensetzung der Unternehmensführung;

c. Daten über Interessenbindungen von Mitgliedern der Unternehmensführung;

d. Daten über die Solvenz sowie allfällige Pfändungs- und Konkursverfahren;

e. Daten über die Bezahlung von Steuern und Sozialabgaben;

f. Referenzen aus früheren Beschaffungsverfahren;

g. Daten über Beziehungen des Betriebs zu ausländischen Staaten oder Organisationen und sonstige Abhängigkeiten.

2 Daten betreffend Aufgaben nach Artikel 6 Absatz 1 Buchstabe a des Nachrichtendienstgesetzes vom 25. September 2015[5] erhebt sie beim Nachrichtendienst des Bundes.

3 Die Betriebe müssen der Fachstelle BS:

a. sachdienliche Unterlagen und Daten zur Prüfung der Sachverhalte nach Absatz 1 einreichen;

b. wahrheitsgemäss Auskunft erteilen.

Art. 10 Ausschluss vom Verfahren
(Art. 57 und 58 ISG)

1 Die Auftraggeberin und die Fachstelle BS informieren einander unverzüglich, wenn Anhaltspunkte bestehen, dass einer der in Frage kommenden Betriebe vom Vergabeverfahren ausgeschlossen werden könnte.

2 Die Fachstelle BS führt das Verfahren fort, solange die Auftraggeberin den betreffenden Betrieb nicht vom Vergabeverfahren ausschliesst.

3 Schliesst die Auftraggeberin den Betrieb aus, so wird das Betriebssicherheitsverfahren für diesen Betrieb eingestellt.

5 SR **121**

Art. 11 Informationsaustausch
(Art. 57 und 58 ISG)

Beim Informationsaustausch nach Artikel 10 Absatz 1 stellen sich die Auftraggeberin und die Fachstelle BS unter Vorbehalt der Artikel 70 Absatz 3 und 71 Absatz 1 Buchstabe a ISG gegenseitig alle Informationen und Daten zur Verfügung, die für die Eignungsprüfung oder die Prüfung der Sachverhalte nach Artikel 44 des Bundesgesetzes vom 21. Juni 2019[6] über das öffentliche Beschaffungswesen (BöB) zweckdienlich sind.

4. Abschnitt: Sicherheitskonzept

Art. 12 Betriebssicherheitsbeauftragte

[1] Betriebe, die für die Ausführung des Auftrages in Frage kommen, melden der Fachstelle BS eine Betriebssicherheitsbeauftragte oder einen Betriebssicherheitsbeauftragten sowie eine angemessene Stellvertretung. Sie oder er ist entweder Mitglied der Geschäftsleitung oder handelt in deren direktem Auftrag.

[2] Die oder der Betriebssicherheitsbeauftragte hat folgende Aufgaben:

a. Sie oder er ist Kontaktperson zur Fachstelle BS für sämtliche Belange der Informationssicherheit.

b. Sie oder er sorgt für die Umsetzung des Sicherheitskonzepts.

c. Sie oder er stellt Antrag auf Einleitung des Betriebssicherheitsverfahrens für Subunternehmen, soweit der Betrieb von der Auftraggeberin ermächtigt wurden, einem solchen einen sicherheitsempfindlichen Auftrag zu vergeben.

Art. 13 Mitteilung des Zuschlags
(Art. 59 Abs. 1 ISG)

[1] Die Mitteilung des Zuschlags erfolgt für jedes einzelne mit einem Rahmenvertrag zusammenhängende Auftragsverhältnis gesondert.

[2] Mit der Mitteilung des Zuschlags übermittelt die Auftraggeberin der Fachstelle BS die für die Erstellung des Sicherheitskonzepts notwendigen Informationen.

Art. 14 Inhalt und Prüfung des Sicherheitskonzepts
(Art. 59 Abs. 2 und 3 ISG)

[1] Die Fachstelle BS legt die Vorgaben an das Sicherheitskonzept nach einer Prüfung im Betrieb fest.

[2] Das Sicherheitskonzept definiert die organisatorischen, personellen, technischen und physischen Massnahmen zur Gewährleistung einer risikogerechten Ausführung des sicherheitsrelevanten Auftrags.

6 SR **172.056.1**

[3] Entspricht das Sicherheitskonzept nicht den Vorgaben der Fachstelle BS, so gewährt diese dem Betrieb eine angemessene Frist zur Verbesserung.

[4] Die Fachstelle BS orientiert die Auftraggeberin, wenn absehbar ist, dass die Prüfung des Sicherheitskonzepts länger als 30 Tage dauert.

Art. 15 Personensicherheitsprüfungen
(Art. 60 ISG)

[1] Die Fachstelle BS legt fest, welche Personen des Betriebs der Personensicherheitsprüfung unterstehen.

[2] Sie kann den Betrieb ermächtigen, die Personensicherheitsprüfung selbstständig einzuleiten.

5. Abschnitt: Betriebssicherheitserklärung und Wiederholung des Verfahrens

Art. 16 Ausstellung der Betriebssicherheitserklärung
(Art. 61 und 62 ISG)

Die Betriebssicherheitserklärung hält fest, für welche sicherheitsempfindliche Tätigkeit der Betrieb zugelassen wird.

Art. 17 Meldungen des Betriebs
(Art. 63 Abs. 2 ISG)

[1] Als sicherheitsrelevante Änderungen gelten insbesondere:

a. Änderung der Eigentumsverhältnisse oder der Unternehmensstrukturen;
b. Änderung des Betriebsstandorts;
c. Änderung in der Zusammensetzung der Unternehmensführung;
d. Änderung der Interessenbindungen von Mitgliedern der Unternehmensführung;
e. Änderung der Solvenz sowie allfällige Pfändungs- und Konkursverfahren;
f. Rechtsstreitigkeiten privat- und öffentlich-rechtlicher Natur sowie Strafverfahren;
g. Änderungen beim Einsatz von Informatikmitteln;
h. Einstellung von Mitarbeitenden, die an sicherheitsempfindlichen Tätigkeiten beteiligt werden sollen;
i. Änderung der Beziehungen des Betriebs zu ausländischen Staaten oder Organisationen und sonstige Abhängigkeiten;
j. Übernahme von Aufträgen, die einen Interessenkonflikt mit oder eine Abhängigkeit von einer Auftraggeberin verursachen.

[2] Als sicherheitsrelevante Vorfälle gelten insbesondere:

a. der widerrechtliche Zutritt zum Betrieb;

b. die missbräuchliche Verwendung der Informatikmittel des Betriebs;

c. ein versuchter oder erfolgreicher Angriff gegen die Informatikmittel des Betriebs;

d. die Entdeckung von Schwachstellen und Sicherheitslücken;

e. die Eröffnung von Schuldbetreibungs- und Strafverfahren gegen Personen des Betriebs, die an der Ausführung des sicherheitsempfindlichen Auftrags beteiligt sind;

f. Hausdurchsuchungen und Beschlagnahmen.

3 Liegen konkrete Anhaltspunkte vor, dass sich ein Vorfall nach Absatz 2 ereignet haben könnte, muss ebenfalls gemeldet werden.

4 Der Betrieb muss auch Änderungen und Vorfälle nach den Absätzen 1 und 2 melden, die Lieferanten betreffen, sofern die Änderungen und Vorfälle für die Erfüllung des sicherheitsempfindlichen Auftrages relevant sein könnten.

5 Er informiert die Fachstelle BS unverzüglich, wenn absehbar ist, dass im Zeitpunkt des Ablaufs der Gültigkeit der Betriebssicherheitserklärung ein sicherheitsempfindlicher Auftrag hängig ist.

Art. 18 Pflichten der Auftraggeberin

1 Stellt die Auftraggeberin in der Zusammenarbeit mit dem Betrieb eine sicherheitsrelevante Änderung oder einen sicherheitsrelevanten Vorfall nach Artikel 17 fest, so trifft sie die notwendigen Sofortmassnahmen und informiert unverzüglich die Fachstelle BS.

2 Die Auftraggeberin informiert die Fachstelle BS zudem, wenn:

a. sie im Rahmen der Erfüllung des sicherheitsempfindlichen Auftrags Anhaltspunkte für einen Widerruf des Zuschlags im Sinne von Artikel 44 BöB hat;

b. sie eine sicherheitsrelevante Änderung des Auftrags vornehmen will;

c. sie beabsichtigt, dem Betrieb einen weiteren Auftrag zu erteilen.

Art. 19 Internationale Betriebssicherheitsbescheinigung
(Art. 66 ISG)

1 Für die Ausstellung einer internationalen Betriebssicherheitsbescheinigung erhebt die Fachstelle BS eine Gebühr von 100 Franken

2 Eine Gebühr nach Zeitaufwand wird zusätzlich erhoben, wenn für die Ausstellung der internationalen Betriebssicherheitsbescheinigung zuerst ein Betriebssicherheitsverfahren durchgeführt werden muss. Es gilt ein Stundenansatz von 100–400 Franken. Dieser richtet sich namentlich nach der Dringlichkeit des Geschäfts und der Funkti-

onsstufe des ausführenden Personals. Im Übrigen gilt die Allgemeine Gebührenverordnung vom 8. September 2004[7].

3 Die Fachstelle des Bundes für Informationssicherheit und die Fachstelle BS können der ausländischen Behörde oder internationalen Organisation auf Anfrage eine Kopie der internationalen Betriebssicherheitsbescheinigung übermitteln.

Art. 20 Widerruf der Betriebssicherheitserklärung und Rückzug des Auftrags
(Art. 67 ISG)

1 Hat die Fachstelle BS Anhaltspunkte, dass ein Grund für den Widerruf der Betriebssicherheitserklärung vorliegt, so setzt sie dem Betrieb nach Rücksprache mit der Auftraggeberin eine Frist zur Behebung der Mängel.

2 Wird der Auftrag infolge des Widerrufs der Betriebssicherheitserklärung zurückgezogen, so sorgt die Auftraggeberin unverzüglich dafür, dass:

a. alle sicherheitsempfindlichen Tätigkeiten sofort eingestellt und die entsprechenden Zugriffsrechte entzogen werden;

b. sämtliche klassifizierten Informationen, Informatikmittel und Materialien sichergestellt werden.

3 Die Auftraggeberin bestätigt der Fachstelle BS innerhalb von zehn Tagen, nachdem sie über den Widerruf informiert wurde, den Vollzug der Massnahmen nach Absatz 2.

Art. 21 Wiederholung des Verfahrens
(Art. 68 ISG)

1 Die Fachstelle BS ist für die Einleitung der Wiederholung des Betriebssicherheitsverfahrens zuständig.

2 Ist im Zeitpunkt des Ablaufs der Gültigkeit der Betriebssicherheitserklärung das Wiederholungsverfahren hängig, so verlängert sich die Gültigkeit, bis eine neue Betriebssicherheitserklärung verfügt oder das Betriebssicherheitsverfahren eingestellt wird.

3 Wird eine Betriebssicherheitserklärung nicht erneuert oder wird das Betriebssicherheitsverfahren eingestellt, so ist Artikel 20 sinngemäss anwendbar. Artikel 58 Absatz 3 ISG bleibt vorbehalten.

6. Abschnitt: Bearbeitung von Personendaten

Art. 22 Informationssystem zum Betriebssicherheitsverfahren
(Art. 70 ISG)

Die im Informationssystem zum Betriebssicherheitsverfahren enthaltenen Personen- und Firmendaten sind im Anhang aufgeführt.

7 SR **172.041.1**

Art. 23 Periodische Kontrolle der Bearbeitung von Personendaten
(Art. 73 Bst. e ISG)

Das [zuständige Departement] sorgt dafür, dass eine von der Fachstelle BS unabhängige Stelle mindestens alle fünf Jahre die rechtmässige Bearbeitung der Personendaten durch die beteiligten Stellen prüft.

7. Abschnitt: Schlussbestimmungen

Art. 24 Aufhebung und Änderung bisherigen Rechts

1 Die Geheimschutzverordnung vom 29. August 1990[8] wird aufgehoben.

2 Die Verordnung vom 24. Juni 2009[9] über internationale militärische Kontakte wird wie folgt geändert:

Art. 5 Abs. 1 Bst d

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 richtet sich nach den entsprechenden Informationsschutzvorschriften, insbesondere:

d. der Verordnung vom …[10] über das Betriebssicherheitsverfahren.

3 Die Nachrichtendienstverordnung vom 16. August 2017[11] wird wie folgt ergänzt:

Anhang 3 Ziffer 10.6

Der NDB kann den folgenden inländischen Behörden und Amtsstellen Personendaten unter den in Artikel 60 NDG genannten Voraussetzungen zu den nachstehend aufgeführten Zwecken bekanntgeben:

10. dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport:

10.5. der Fachstelle für Personensicherheitsprüfungen: zur Durchführung von Personensicherheitsprüfungen,

10.6. der Fachstelle Betriebssicherheit: zur Durchführung von Betriebssicherheitsverfahren;

4 Die Verordnung vom 21. November 2018[12] über die Militärische Sicherheit wird wie folgt geändert:

Art. 3 Bst. b

Aufgehoben

8 AS **1990** 1774
9 SR **510.215**
10 SR ….
11 SR **121.1**
12 SR **513.61**

Art. 6 Abs. 2 Bst. e und f

[2] Sie erfüllt folgende Aufgaben:

e. Sie führt im VBS und in der Armee in diesen Bereichen ein fachspezifisches Controlling durch und regelt die dafür erforderlichen Meldepflichten.

f. Sie verfügt über Kontrollrechte im VBS und in der Armee.

[5] Die Verordnung vom 16. Dezember 2009[13] über die militärischen Informationssysteme wird wie folgt geändert:

Art. 68 und Anhang 31

Aufgehoben

Art. 25 Übergangsbestimmungen

Für Aufträge, die vor Inkrafttreten dieser Verordnung erteilt wurden, sowie für Geheimschutzverfahren, die im Zeitpunkt des Inkrafttretens dieser Verordnung hängig sind, gilt das bisherige Recht.

Art. 26 Inkrafttreten

Diese Verordnung tritt am … 2023 in Kraft.

… Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Ignazio Cassis
Der Bundeskanzler: Walter Thurnherr

13 SR **510.911**

Anhang
(Art. 22)

Daten des Informationssystems zum Betriebssicherheitsverfahren

Personendaten

1. Name
2. Vorname
3. Adresse
4. Versichertennummer
5. Nationalität
6. Heimatort
7. Arbeitgeber und dessen Adresse
8. Zivilstand
9. Geburtsort
10. Geburtsdatum
11. Datum der Einbürgerung
12. Aufenthalt in der Schweiz seit
13. Name und Vorname des Ehepartners oder der Ehepartnerin bzw. des Lebenspartners oder der Lebenspartnerin
14. Funktion
15. Auftraggeberin und deren Adresse
16. Projekt

Firmendaten

Firma

17. Dossiernummer
18. Name
19. Adresse
20. Telefon
21. Fax
22. E-Mail-Adresse
23. Internetadresse

Betriebssicherheitsbeauftragte

24. Anrede
25. Name

26. Vorname
27. Geschlecht
28. E-Mail-Adresse

Prüfungsdaten

29. Datum der Eignungsprüfung
30. Branchencode zur wirtschaftlichen Tätigkeit der Firma (NOGA-Code)
31. Besuch (Datum, chronologisch mit Textvermerk)
32. Kontrolle (Datum, chronologisch mit Textvermerk)
33. Betriebssicherheitserklärung (Datum, Ausstellung, Widerruf, Rückgabe)
34. Sicherheitskonzept (Datum chronologisch)

Akten

35. Exemplarnummer
36. Absender/in
37. Aktendatum
38. Versanddatum
39. Kontrolldatum
40. Rückgabedatum
41. Bezeichnung

Aufträge

42. Bezeichnung (Hauptauftrag)
43. Auftraggeberin
44. Bezeichnung (Aufträge)
45. Klassifizierung
46. Meldungsdatum
47. Gültigkeitsbeginn
48. Gültigkeitsende
49. Kurzbezeichnung (Branche)
50. Branchencode zur wirtschaftlichen Tätigkeit der Firma (NOGA-Code)