Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verordnung über die abschliessende Inkraftsetzung des Informationssicherheitsgesetzes vom 18. Dezember 2020

vom …

Der Schweizerische Bundesrat,

gestützt auf Artikel 92 Absatz 2 des Informationssicherheitsgesetzes vom 18. Dezember 2020[1] (ISG),

verordnet:

Einziger Artikel

Das Informationssicherheitsgesetz vom 18. Dezember 2020 tritt am 1. Januar 2024 abschliessend in Kraft.

…

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Alain Berset
Der Bundeskanzler: Walter Thurnherr

1 SR **128**; bereits in Kraft gesetzte Bestimmungen: AS **2022** 232, 503 und 750

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

vom ...

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 das Bundesgesetz vom 17. März 2023[3] über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG),
auf das Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997[4] (RVOG),
auf Artikel 27 Absätze 5 und 6 des Bundespersonalgesetzes vom 24. März 2000[5] und auf Artikel 186 des Bundesgesetzes vom 3. Oktober 2008[6] über militärische und andere Informationssysteme im VBS,

Art. 2 Geltungsbereich

[1] Die Artikel 24 und 25 ISG sowie diese Verordnung gelten für:

1 SR **172.010.59**
2 SR **128**
3 SR **…**
4 SR **172.010**
5 SR **172.220.1**
6 SR **510.91**

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

b. die Armee.

2 Die Geltung dieser Verordnung für die Verwaltungseinheiten der dezentralen Bundesverwaltung nach Artikel 2 Absatz 3 RVOG und Organisationen nach Artikel 2 Absatz 4 RVOG richtet sich nach Artikel 2 Absätze 2 Buchstabe b und 3 der Informationssicherheitsverordnung vom ...[8].

Art. 5 IAM-Systeme

1 Die folgenden Bundesorgane sind für die nachstehenden IAM-Systeme der zentralen Bundesverwaltung verantwortlich:

a. der Bereich digitale Transformation und IKT-Lenkung der Bundeskanzlei (Bereich DTI der BK) für:
   1. alle als Standarddienste angebotenen oder dem Bereich DTI der BK ausdrücklich zugewiesenen IAM-Systeme einschliesslich derer Zurverfügungstellung an Kantone und Gemeinden sowie Organisationen und Personen des öffentlichen oder privaten Rechts nach Artikel 11 Absatz 3 EMBAG,
   2. das IAM-System der Supportprozesse Finanzen, Beschaffung, Immobilien und Logistik einschliesslich der Cloud-Anbindungen;

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

c. das Generalsekretariat des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport für die von der Gruppe Verteidigung (Gruppe V) betriebenen IAM-Systeme;

d. die Eidgenössische Finanzverwaltung für das in der zentralen Ausgleichsstelle betriebene IAM-System zur Versorgung der Sozialversicherungssysteme der 1. Säule und deren Prozessunterstützung;

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 Sie sorgen dafür, dass die Bearbeitung der Personendaten in den IAM-Systemen, für die sie verantwortlich sind, mindestens alle vier Jahre von einer externen Stelle überprüft wird.

3 Die folgenden Organe sind für die nachstehenden IAM-Systeme verantwortlich:

7 SR **172.010.1**
8 SR **...**

a. die Gruppe V für die IAM-Systeme der Armee;

b. die jeweiligen Verwaltungseinheiten für die IAM-Systeme der Verwaltungseinheiten der dezentralen Bundesverwaltung;

c. die jeweiligen Organisationen für die IAM-Systeme der Organisationen nach Artikel 2 Absatz 4 RVOG.

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

5 Die Verantwortung für das nachgelagerte System, insbesondere für den Zugang dazu, bleibt bei der Fachstelle, die für dieses zuständig ist.

Art. 6 Bst. b Ziff. 3

Die für Verzeichnisdienste ausserhalb von IAM-Systemen verantwortlichen Bundesorgane sind:

b. für die anderen Verzeichnisse: die Informatik-Leistungserbringer, die diese Systeme betreiben, im Einzelnen:

3. die Gruppe V,

Art. 7 Bst. b

Die betroffenen Personen machen ihre Rechte in Bezug auf IAM-Systeme und Verzeichnisdienste bei den folgenden Stellen geltend:

b. ihr Berichtigungs- und Vernichtungsrecht:

1. beim Personaldienst ihrer Verwaltungseinheit oder ihrer Organisation oder bei der sonst für die Nachführung ihrer Daten zuständigen Stelle,

2. im Falle von Artikel 9 Buchstabe b: bei den verantwortlichen Organen.

Art. 9 Bst. b

In den IAM-Systemen können, zusätzlich zu den Daten nach Artikel 8, Daten der folgenden Personen bearbeitet werden:

b. von Privatpersonen und Vertreterinnen oder Vertretern von Organisationen, die auf vom Bund oder, für den Vollzug von kantonalem Recht, von Kantonen und Gemeinden sowie Organisationen und Personen des öffentlichen oder privaten Rechts bereitgestellte Informationssysteme, wie E-Government-Anwendungen, zugreifen.

Art. 11 Abs. 2 und 3

2 Es darf in diesen Systemen kein Profiling nach Artikel 5 Buchstaben f und g des Datenschutzgesetzes vom 25. September 2020[9] durchgeführt werden.

9 SR **235.1**

3 Es dürfen in diesen Systemen, sofern hierfür keine besondere rechtliche Grundlage besteht, keine besonders schützenswerten Personendaten bearbeitet werden. Davon ausgenommen ist die Bearbeitung biometrischer Daten durch IAM-Systeme zur risikogerechten Identifizierung von Personen nach den Artikeln 8 und 9 Buchstabe a (Art. 20 Abs. 2 ISG).

Art. 12 Abs. 4

4 Sie können Daten von externen Personen automatisch von externen IAM-Systemen beziehen, die nach den Artikeln 21–24 mit den IAM-Systemen des Bundes verbunden sind.

Art. 13 Abs. 4 Bst. a

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 6 der Datenschutzverordnung vom 31. August 2022[10] (DSV) 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 nach dieser Verordnung verantwortliche Organ eines Systems oder Verzeichnisdiensts ein Bearbeitungsreglement nach Artikel 6 DSV[11].

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 Minimalanforderungen bezüglich der Informationssicherheit erfüllen.

10 SR **235.11**
11 SR **235.11**

Art. 20 IAM-Gesamtsystem

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

Art. 21 Einleitungssatz und Bst. a

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 oder im Falle der Kantone diese eine mindestens gleichwertige Informationssicherheit gewährleisten:

a. IAM-Systeme mit kantonalen und kommunalen Mitarbeiterinnen und Mitarbeitern nach Artikel 9 Buchstabe a sowie IAM-Systeme des Fürstentums Liechtenstein;

Art. 24 Abs. 1 Bst. a

1 IAM-Systeme des Bundes können als Lieferant von Identitäts- und Authentifizierungsinformationen an ein externes IAM-System oder einen externen Identitätsverbund angeschlossen werden, wenn die folgenden Voraussetzungen erfüllt sind:

a. Der Anschluss dient dazu, Personen nach Artikel 8 oder 9 den Zugang:
   1. zu im Auftrag des Bundes von Externen betriebenen Informationssystemen oder zu fremden Informationssystemen zu gewähren, auf die sie zur Erfüllung ihrer gesetzlichen Aufgaben zugreifen müssen, oder
   2. zu für den Vollzug von kantonalem Recht von Kantonen und Gemeinden sowie Organisationen und Personen des öffentlichen oder privaten Rechts bereitgestellten Informationssystemen, wie E-Government-Anwendungen, zu gewähren.

II

Der Anhang erhält die neue Fassung gemäss Beilage.

III

Diese Verordnung tritt am 1. Januar 2024 Kraft.

… Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Alain Berset
Der Bundeskanzler: Walter Thurnherr

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

Datenkategorien

Vorbemerkung: Zur Bedeutung der Sterne (*) siehe Artikel 11 Absatz 4.

	Verzeichnisdienste	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	x
2. Vornamen*	x	x	x
3. Geburtsdatum		x	x
4. Geburtsort			x
5. Nationalität			x
6. Geschlecht		x	x
7. Anrede*	x	x	x
8. Titel*	x	x	x
9. Initialen*	x	x	x
10. lokale Personenidentifikatoren	x	x	x
11. Berufsbezeichnung*	x	x	x
12. Korrespondenzsprache*	x	x	x
13. besondere biometrische Personenmerkmale, insbesondere Irisbild, Retina, Venenscan, Fingerabdruck, Handabdruck, Gesichtsformmerkmale und Stimmprofil		x	
14. Gesichtsbild	x	x	x
15. AHV-Nummer	x	x	x
b. Angaben zum Verhältnis zum Arbeit-/Auftraggeber			
1. Anstellungsverhältnis (intern/extern)*	x	x	
2. Informationen zur Organisation und zu den Planstellen*	x	x	x
3. künftige Zuordnung zu einer Organisationseinheit	x	x	
4. Personalkategorie		x	
5. Personalnummer (auch kantonale)	x	x	
6. Funktion*	x	x	
7. Stellenbezeichnung*	x	x	
8. Kennung des Personalinformationssystems (Quelle)	x	x	

	Verzeichnisdienste	IAM-Systeme mit Personen nach Art. 8 und 9 Bst. a	IAM-Systeme mit Personen nach Art. 9 Bst. b
9. Eintritts- und Austrittsdatum	x	x	
10. Ausweis- und/oder Badgenummer	x	x	x
c. Kontaktangaben			
1. Arbeitsort und geschäftliche Postadresse*	x	x	x
2. private Postadresse			x
3. Büronummer*	x	x	
4. geschäftliche Adressierungselemente* wie E-Mail-Adresse*, Telefonnummern*, Faxnummer*, VOIP-Adresse*	x	x	x
5. externe Adressierungselemente* (für Mitarbeiter/innen und Beauftragte*) oder private Adressierungselemente	x	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	x
2. Adressierungselemente, Kennnummern usw.	x		
3. Systemsprache der Geräte, Anschlüsse usw.	x	x	x
4. öffentliche Schlüssel der digitalen Zertifikate*	x	x	x
5. Berechtigungsgruppen	x	x	x
6. Namen für die Anmeldung an den IT-Systemen	x	x	x
7. Passwörter (kryptographisch gesichert)		x	x
8. letztes Login		x	x
9. fehlgeschlagene Login-Versuche		x	x
10. Status (aktiv/passiv)		x	x
11. Authentisierungsqualität		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 Informationssicherheit in der Bundesverwaltung und der Armee

(Informationssicherheitsverordnung, ISV)

vom …

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 ISG)

[1] Diese Verordnung gilt für:

a. den Bundesrat;

b. die Departemente;

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

d. die Armee.

[2] Für Verwaltungseinheiten der dezentralen Bundesverwaltung nach Artikel 2 Absatz 3 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[2]

1 SR **128**
2 SR **172.010**

(RVOG) und Organisationen nach Artikel 2 Absatz 4 RVOG gelten die folgenden Bestimmungen des ISG und der vorliegenden Verordnung:

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

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

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

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

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

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

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

2. Abschnitt: Grundsätze

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

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

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

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

3 SR **172.010.58**

Art. 4 Verantwortung

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

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

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

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

3. Abschnitt: Management der Informationssicherheit

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

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

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

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

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

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

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

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

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

2 Als Schutzobjekte gelten einzelne oder mehrere gleichartige oder zusammenhängende:

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

b. Informatikmittel nach Artikel 5 Buchstabe a ISG.

3 Im Inventar ist festzuhalten:

a. der Schutzbedarf der Schutzobjekte;

b. die Verantwortlichkeiten für die Schutzobjekte;

c. die Beteiligung von Dritten;

d. das Ergebnis der Risikobeurteilung;

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

f. die periodischen Kontrollen und Audits;

g. gegebenenfalls: die geteilte Nutzung der Schutzobjekte.

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

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

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

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

c. Sie kontrollieren die Einhaltung der Vorgaben.

d. Sie weisen die Akzeptanz der Restrisiken nach.

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

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

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

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

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

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

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

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

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

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

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

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

2 Inhalt der Schulungen ist insbesondere:

a. die korrekte Identifizierung des Schutzbedarfs von Informationen;

b. der sichere Umgang mit Informationen und Informatikmitteln;

c. die korrekte Reaktion bei Verdacht auf einen Sicherheitsvorfall;

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

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

e. die Kontrollaufgaben der Vorgesetzten;

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

3 Die Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c, die Departemente und die Fachstelle des Bundes für Informationssicherheit sorgen für die regelmässige Sensibilisierung der Mitarbeitenden aller Stufen in Bezug auf die Risiken der Informationssicherheit.

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

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

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

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

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

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

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

a. Die Funktionsfähigkeit der Bundesverwaltung könnte gefährdet sein.

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

c. Es könnten mehrere Departemente betroffen sein.

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

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

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

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

7 Sie kann in Fällen nach Absatz 5 nach Rücksprache mit der betroffenen Verwaltungseinheit und dem betroffenen Departement die Federführung für die Bewältigung eines Sicherheitsvorfalls oder die Behandlung einer Sicherheitslücke übernehmen oder diese mit deren Zustimmung dem BACS übertragen. Dabei haben sie folgende Aufgaben und Kompetenzen:

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

b. Sie können Sofortmassnahmen anordnen.

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

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

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

Art. 13 Planung von Kontrollen und Audits

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

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

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

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

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

Art. 14 Berichterstattung
(Art. 7 Abs. 1, 81 Abs. 2 Bst. c und 83 Abs. 1 Bst. h ISG)

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

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

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

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

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

4. Abschnitt: Klassifizierte Informationen

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

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

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

Art. 17 Klassifizierende Stellen
(Art. 12 ISG)

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

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

3 Sie legt nach der Konsultation der Konferenz der Informationssicherheitsbeauftragten in generell-abstrakten Weisungen mit Geltung für alle Organisationen nach Arti-

6 SR **172.010.58**

kel 2 Absätze 1–3 fest, wie Informationen, die departementsübergreifend häufig bearbeitet werden, zu klassifizieren sind und wie lange die Klassifizierung dauern soll.

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

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

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

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

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

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

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

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

c. Einzelne Personen sind körperlich verletzt.

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

e. Die Schweiz ist aussenpolitisch oder wirtschaftlich benachteiligt.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2 Sie hört vorgängig die folgenden Stellen an:

a. das BACS;

b. den kryptografischen Dienst der Armee;

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

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

3 Die BK regelt die Bearbeitung klassifizierter Bundesratsgeschäfte.

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

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

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

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

b. die Direktorin oder der Direktor des NDB;

c. die Chefin oder der Chef der Armee;

d. die Chefin oder der Chef des Kommandos Operationen;

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

7 SR **172.056.15**

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

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

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

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

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

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

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

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

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

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

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

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

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

8 SR **172.056.15**

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

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

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

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

5. Abschnitt: Sicherheit beim Einsatz von Informatikmitteln

Art. 27 Sicherheitsverfahren
(Art. 16 ISG)

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

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

[3] Sie weisen Restrisiken aus.

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

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

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

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

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

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

9 SR **152.11**

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

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

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

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

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

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

b. Informatikmittel der Sicherheitsstufe «sehr hoher Schutz».

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

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

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

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

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

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

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

6. Abschnitt: Personelle Massnahmen und physischer Schutz

Art. 31 Prüfung der Identität von Personen und Maschinen

(Art. 20 und 85 ISG)

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

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

Art. 32 Personensicherheit

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

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

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

Art. 33 Verdacht auf strafbares Verhalten

(Art. 7 Abs. 2 Bst. c ISG)

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

10 SR **172.010.442**
11 SR **172.010.59**
12 SR **128.xxx**

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

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

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

2 Sie berücksichtigt dabei:

a. den gesamten Lebenszyklus der Informationen und Informatikmittel;

b. die arbeitsplatzspezifischen Anforderungen;

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

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

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

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

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

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

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

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

7. Abschnitt: Sicherheitsorganisation

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

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

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

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

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

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

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

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

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

a. sie über angemessene Kompetenzen und Ressourcen verfügen; und

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

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

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

2 Die Informationssicherheitsbeauftragten haben insbesondere folgende Aufgaben und Kompetenzen:

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

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

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

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

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

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

g. Sie stellen Antrag auf Einleitung des Betriebssicherheitsverfahrens nach Artikel 4 VBSV[13].

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

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

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

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

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

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

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

13 SR **128.xxx**
14 SR **172.010.58**

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

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

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

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

2 Sie haben dabei insbesondere folgende Aufgaben:

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

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

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

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

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

f. Sie beauftragen ihre Informationssicherheitsbeauftragten nach Artikel 40 und sorgen dafür, dass:
   1. sie über angemessene Kompetenzen und Ressourcen verfügen;
   2. ihnen keine Aufgaben übertragen werden, die einen Interessenkonflikt mit ihren Aufgaben nach Artikel 40 zur Folge haben können.

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

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

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

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

a. Sie sorgen für die departementsübergreifende Koordination der Informationssicherheit.

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

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

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

e. Sie vertreten das Departement in Fachgremien.

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

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

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

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

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

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

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

a. Sie erarbeitet Strategien zu sicherheitsrelevanten Themen.

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

c. Sie wirkt bei der Ausbildung der Sicherheitsorganisation mit.

d. Sie stellt Vorlagen und Hilfsmittel bereit.

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

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

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

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

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

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

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

d. Sie vertritt die Schweiz in internationalen Fachgremien.

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

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

4 Sie ist Teil des Staatssekretariats für Sicherheitspolitik im VBS.

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

1 Das BACS hat folgende Aufgaben und Kompetenzen:

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

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

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

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

8. Abschnitt: Kosten und Evaluation

Art. 44 Kosten

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

15 SR ...

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

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

Art. 45 Evaluation
(Art. 88 ISG)

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

9. Abschnitt: Bearbeitung von Informationen und Personendaten

Art. 46 Allgemeines

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

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

a. dies zur Gewährleistung der Informationssicherheit zweckmässig ist;

b. keine gesetzlichen oder vertraglichen Geheimhaltungspflichten verletzt werden;

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

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

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

4 Werden bei einem Sicherheitsvorfall beim Bund oder bei Dritten, die mit dem Bund zusammenarbeiten, Informationen des Bundes entwendet und im Internet veröffent-

16 SR **128.xxx**
17 SR **235.1**

licht, so dürfen sie die Informationen herunterladen und analysieren, um die Betroffenheit des Bundes zu beurteilen und die nötigen Schutzmassnahmen zu ergreifen. Sie dürfen Daten, die für die Beurteilung nicht relevant sind, nicht bearbeiten.

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

Art. 47 ISMS-Anwendung

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

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

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

Art. 48 Elektronische Formulardienste

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

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

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

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

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

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

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

18 SR **128.xxx**

10. Abschnitt: Schlussbestimmungen

Art. 49 Besondere Vollzugsbestimmungen

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

Art. 50 Aufhebung und Änderung anderer Erlasse

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

Art. 51 Übergangsbestimmungen

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

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

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

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

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

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

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

Art. 52 Inkrafttreten

Diese Verordnung tritt am 1. Januar 2024 in Kraft.

… Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Alain Berset
Der Bundeskanzler: Walter Thurnherr

Anhang 1
(Art. 48)

Datenbearbeitung mit den elektronischen Formulardiensten

Mit den folgenden Formulardiensten dürfen nachstehende Personendaten bearbeitet werden:

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

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

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

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

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

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

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

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

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

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

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

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

b. Angaben zur Betriebssicherheitserklärung:
   1. Ausstellungsdatum und Gültigkeitsdauer*
   2. Anwendungsbereich und Auflagen*

3. Höchste zugelassene Klassifizierungs- oder Sicherheitsstufe*

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

4. Formulardienst nach Artikel 48 Absatz 3

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

Anhang 2
(Art. 50)

Aufhebung und Änderung anderer Erlasse

I

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

II

Die nachstehenden Erlasse werden wie folgt geändert:

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

Art. 9 Abs. 7

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

Art. 13 Abs. 1 Bst. b

1 Für die Gewährleistung der Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom ...[21].

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

Art. 13 Abs. 1 Bst. b und c

1 Für die Gewährleistung der Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom ...[23].

c. *Aufgehoben*

19 [AS **2020** 2107, **2020** 5871, **2021** 132]
20 SR **120.52**
21 SR **...**
22 SR **121.2**
23 SR **...**

Art. 15 Datenübermittlung ausserhalb von SiLAN

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

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

Art. 20 Abs. 2 Bst. b

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

b. der Informationssicherheitsverordnung vom ...[26].

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

Art. 12 Bst. b

Die Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom ...[28];

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

Art. 34 Bst. b

Die Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom ...[30];

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

Art. 17 Sachüberschrift und Abs. 1 Bst. b

Daten- und Informationssicherheit

[1] Die Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom ...[32].

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

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

Art. 41 Abs. 2 Bst. b

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

b. der Informationssicherheitsverordnung vom ...[34].

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

Art. 11 Bearbeitung von klassifizierten Informationen

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

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

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

Art. 3 Sichere Aufbewahrung

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

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

3. Abschnitt Sachüberschrift

3. Abschnitt: Datenschutz und Informationssicherheit

Art. 11 Abs. 1 Einleitungssatz und Bst. b

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

33 SR **172.010.21**
34 SR **...**
35 SR **172.010.441**
36 SR **...**
37 SR **172.010.442**
38 SR **...**
39 SR **172.211.21**

b. der Informationssicherheitsverordnung vom ...[40].

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

3. Abschnitt Sachüberschrift

3. Abschnitt: Datenschutz und Informationssicherheit

Art. 12 Abs. Einleitungssatz und Bst. b

1 Die Daten- und die Informationssicherheit richten sich nach:

b. der Informationssicherheitsverordnung vom ... [42].

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

Art. 14 Abs. 1 Einleitungssatz und Bst. b

1 Die Daten- und Informationssicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom ... [44];

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

Art. 4 Abs. 2

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

Art. 12 Abs. 4

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

Art. 15 Abs. 1 Bst. b

1 Für die Gewährleistung der Datensicherheit gelten:

40 SR **...**
41 SR **172.220.111.42**
42 SR ...
43 SR **235.22**
44 SR **...**
45 SR **312.21**
46 SR ...
47 SR ...

b. die Informationssicherheitsverordnung vom ... [48];

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

Art. 18 Abs. 1

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

15. Strafregisterverordnung vom 19. Oktober 2022[52]

Art. 11 Abs. 1 Bst. b

[1] Für die Gewährleistung der Datensicherheit gelten namentlich:

b. die Informationssicherheitsverordnung vom ... [53].

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

Gliederungstitel vor Art. 13

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

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

Daten- und Informationssicherheit

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

b. der Informationssicherheitsverordnung vom ... [55].

48 SR **...**
49 SR **313.041**
50 SR **235.11**
51 SR ...
52 SR **331**
53 SR **...**
54 SR **351.12**
55 SR **...**

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

Art. 26 Bst. b

Für die Gewährleistung der Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom ... [57] (ISV).

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

[1] Für die Gewährleistung der Datensicherheit gelten:

b. die ISV[58].

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

[1] Für die Gewährleistung der Datensicherheit gelten:

b. die ISV[59].

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

Ersatz eines Ausdrucks

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

Art. 9 Abs. 5

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

Art. 14 Abs. 2 Bst. b

[2] Die Datensicherheit richtet sich nach:

b. die Informationssicherheitsverordnung vom ...[62].

56 SR **360.2**
57 SR ...
58 SR ...
59 SR ...
60 SR **361.0**
61 SR ...
62 SR ...

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

Art. 12 Bst. b

Für die Gewährleistung der Datensicherheit gelten:

b. der Informationssicherheitsverordnung vom ... [64].

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

Art. 14 Bst. b

Die Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom ... [66].

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

Art. 12 Abs. 1 Bst. b

[1] Für die Gewährleistung der Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom ... [68].

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

Art. 53 Abs. 1 Bst. b

[1] Die Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom ...[70];

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

Art. 19 Abs. 1 Bst. b

[1] Die Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom ... [72].

63 SR **361.2**
64 SR ...
65 SR **361.3**
66 SR ...
67 SR **361.4**
68 SR ...
69 SR **362.0**
70 SR **...**
71 SR **363.1**
72 SR **...**

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

Art. 21 Abs. 1 Einleitungssatz und Bst. b

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

b. der Informationssicherheitsverordnung vom ... [74].

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

Art. 10 Abs. 2

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

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

Art. 18 Abs. 1 Bst. b

[1] Für die Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom ... [78].

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

Art. 15 Abs. 1 Bst. b

[1] Für die Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom ... [80].

73 SR **412.108.1**
74 SR **...**
75 SR **431.011**
76 SR **...**
77 SR **431.841**
78 SR ...
79 SR **431.903**
80 SR ...

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

Art. 24 Informationssicherheit

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

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

Ersatz eines Ausdrucks

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

Art. 20 Abs. 1

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

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

Art. 4 Bst. c

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

c. die Fachstelle des Bundes für Informationssicherheit;

Art. 5 Abs. 1

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

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

81 SR **453.2**
82 SR ...
83 SR **455.61**
84 SR ...
85 SR **510.215**
86 SR **128**

b. der Verordnung vom …[87] über die Personensicherheitsprüfungen;

c. der Informationssicherheitsverordnung vom …[88];

d. der Verordnung über das Betriebssicherheitsverfahren vom …[89].

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

Art. 7 Abs. 1

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

32. Waffenverordnung vom 2. Juli 2008[92]

Art. 66c Abs. 1 Bst. b

[1] Die Gewährleistung der Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom ... [93].

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

Art. 8 Abs. 2 Bst. b

[2] Im Übrigen gelten:

b. die Informationssicherheitsverordnung vom ... [95].

87 SR **...**
88 SR **...**
89 SR **...**
90 SR **510.292**
91 SR ...
92 SR **514.541**
93 SR ...
94 SR **531.215.32**
95 SR ...

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

Art. 4 Abs. 5

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

Art. 7 Abs. 4

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

Art. 8 Abs. 5

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

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

Art. 12 Abs. 1

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

36. Energieverordnung vom 1. November 2017[103]

Art. 2 Abs. 2 Bst. d

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

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

96 SR **531.32**
97 SR ...
98 SR ...
99 SR ...
100 SR **631.061**
101 SR **235.11**
102 SR ...
103 SR **730.01**
104 SR ...

37. Organzuteilungsverordnung vom 16. März 2007[105]

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

Datensicherheit

[1] Für die Gewährleistung der Datensicherheit gelten:

b. der Informationssicherheitsverordnung vom ...[106].

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

Art. 15 Informationssicherheit

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

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

Art. 11 Abs. 1 Bst. b

[1] Die Datensicherheit richtet sich nach:

b. der Informationssicherheitsverordnung vom ...[110];

40. Familienzulagenverordnung vom 31. Oktober 2007[111]

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

Datenschutz und Informationssicherheit

[1] Der Datenschutz und die Informationssicherheit richten sich nach:

b. der Informationssicherheitsverordnung vom ... [112];

105 SR **810.212.4**
106 SR ...
107 SR **812.214.4**
108 SR ...
109 SR **824.095**
110 SR ...
111 SR **836.21**
112 SR ...

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

Art. 102g Informationssicherheit

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

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

Art. 9 Abs. 1 Einleitungssatz und Bst. b

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

b. der Informationssicherheitsverordnung vom ... [116].

43. Edelmetallkontrollverordnung vom 8. Mai 1934[117]

Art. 34e

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

Art. 34g Abs. 1

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

44. Sprengstoffverordnung vom 27. November 2000[121]

Art. 117j Abs. 1 Bst. b

[1] Für die Gewährleistung der Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom ... [122].

113 SR **916.443.10**
114 SR ...
115 SR **935.412**
116 SR ...
117 SR **941.311**
118 SR **235.1**
119 SR **235.11**
120 SR ...
121 SR **941.411**
122 SR ...

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

Art. 19 Abs. 1 Bst. b

[1] Für die Datensicherheit gelten:

b. die Informationssicherheitsverordnung vom ... [124].

123 SR **955.23**
124 SR ...

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verordnung über das Betriebssicherheitsverfahren (VBSV)

vom …

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 Aufgaben und Zuständigkeiten 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 für:

a. die verpflichteten Behörden nach Artikel 2 Absatz 1 ISG;

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

c. die Armee.

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

[3] Die Geltung dieser Verordnung für die Verwaltungseinheiten der dezentralen Bundesverwaltung nach Artikel 2 Absatz 3 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[3] (RVOG) und Organisationen nach Artikel 2 Absatz 4 RVOG richtet sich nach Artikel 2 Absätze 2 und 3 der Informationssicherheitsverordnung vom …[4] (ISV).

Art. 2 Betroffene Betriebe
(Art. 50 ISG)

[1] Das Betriebssicherheitsverfahren nach dieser Verordnung wird bei Betrieben mit Sitz in der Schweiz durchgeführt.

[2] Die völkerrechtlichen Verträge nach Artikel 87 ISG regeln die Durchführung des Betriebssicherheitsverfahrens für Betriebe mit Sitz im Ausland.

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

[1] Das Staatssekretariat für Sicherheitspolitik im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) betreibt die Fachstelle BS.

[2] Die Fachstelle koordiniert ihre internationalen 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] Im Zuständigkeitsbereich des Bundesrats sind die Informationssicherheitsbeauftragten der Verwaltungseinheiten nach Artikel 37 ISV für den Antrag auf Einleitung des Verfahrens zuständig. Vorbehalten bleibt Artikel 13 Absatz 2 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.

3 SR **172.010**
4 SR **...**

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] Auf die Einleitung des Verfahrens darf nicht verzichtet werden, wenn eine der folgenden Voraussetzungen erfüllt ist:

a. Der sicherheitsempfindliche Auftrag umfasst die Bearbeitung als «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 als «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 informiert 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 beantragt sie der ausländischen Sicherheitsbehörde 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[5] und der Verordnung vom …[6] über die Personensicherheitsprüfungen.

5 SR **…**
6 SR **…**

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 Fällen auf Antrag der Auftraggeberin eine höhere Zahl zulassen.

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 oder 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, die der Nachrichtendienst des Bundes in Erfüllung seiner Aufgabe nach Artikel 6 Absatz 1 Buchstabe a des Nachrichtendienstgesetzes vom 25. September 2015[7] erhoben hat, bezieht sie beim Nachrichtendienst des Bundes.

7 SR **121**

Art. 10 Ausschluss vom Vergabeverfahren
(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.

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[8] über das öffentliche Beschaffungswesen (BöB) zweckdienlich sind.

4. Abschnitt: Sicherheitskonzept

Art. 12 Inhalt und Prüfung des Sicherheitskonzepts
(Art. 59 Abs. 2 und 3 ISG)

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

[2] Die Fachstelle BS legt die Vorgaben an das Sicherheitskonzept nach einem Augenschein im Betrieb fest. Sie berücksichtigt dabei die individuellen Voraussetzungen des Betriebs.

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

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

Art. 13 Betriebssicherheitsbeauftragte

[1] Betriebe, die für die Ausführung des Auftrags in Frage kommen, müssen der Fachstelle BS eine Betriebssicherheitsbeauftragte oder einen Betriebssicherheitsbeauftragten sowie deren oder dessen Stellvertretung melden. Die oder der Sicherheitsbeauf-

8 SR **172.056.1**

tragte sowie deren oder dessen Stellvertretung muss entweder Mitglied der Geschäftsleitung sein oder in deren direktem Auftrag handeln.

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 (Art. 12 Abs. 1).

c. Wird der Betrieb von der Auftraggeberin ermächtigt, einem Subunternehmen einen sicherheitsempfindlichen Auftrag zu vergeben, so stellt sie oder er den Antrag auf Einleitung des Betriebssicherheitsverfahrens für das Subunternehmen.

Art. 14 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. 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 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 Änderung gilt insbesondere:

a. eine Änderung der Eigentumsverhältnisse oder der Unternehmensstrukturen;

b. eine Änderung des Betriebsstandorts;

c. eine Änderung in der Zusammensetzung der Unternehmensführung;

d. eine Änderung der Interessenbindungen von Mitgliedern der Unternehmensführung;

e. eine Änderung der Solvenz sowie ein allfälliges Pfändungs- oder Konkursverfahren;

f. das Vorhandensein von Rechtsstreitigkeiten privatrechtlicher oder öffentlichrechtlicher Natur sowie von Strafverfahren;

g. eine Änderung beim Einsatz von Informatikmitteln;

h. das Einstellen von Mitarbeitenden, die an sicherheitsempfindlichen Tätigkeiten beteiligt werden sollen;

i. eine Änderung der Beziehungen des Betriebs zu ausländischen Staaten oder Organisationen sowie eine Änderung sonstiger Abhängigkeiten;

j. die Übernahme von Aufträgen, die einen Interessenkonflikt mit oder eine Abhängigkeit von einer Auftraggeberin verursachen.

2 Als sicherheitsrelevanter Vorfall gilt 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. das Durchführen von Hausdurchsuchungen und Beschlagnahmen im Betrieb.

3 Der Betrieb muss auch sicherheitsrelevante Änderungen und Vorfälle melden, die Lieferanten betreffen, sofern diese Änderungen und Vorfälle für die Erfüllung des sicherheitsempfindlichen Auftrags relevant sein könnten.

4 Er muss die Fachstelle BS unverzüglich informieren, 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 fest, so trifft sie die notwendigen Sofortmassnahmen und informiert unverzüglich die Fachstelle BS.

2 Die Auftraggeberin informiert die Fachstelle BS zudem, wenn sie:

a. im Rahmen der Erfüllung des sicherheitsempfindlichen Auftrags Anhaltspunkte für einen Widerruf des Zuschlags im Sinne von Artikel 44 BöB[9] hat;

9 SR **172.056.1**

b. eine sicherheitsrelevante Änderung des Auftrags vornehmen will;

c. 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 Funktionsstufe des ausführenden Personals. Im Übrigen gilt die Allgemeine Gebührenverordnung vom 8. September 2004[10].

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 Be-

10 SR **172.041.1**

triebssicherheitserklärung 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 1 aufgeführt.

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

Das VBS 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: Leistungen der Fachstelle BS zugunsten der Kantone
(Art. 86 Abs. 4 ISG)

Art. 24

1 Die Kantone können für sicherheitsempfindliche Aufträge nach kantonalem Recht bei der Fachstelle BS die Durchführung einer Beurteilung der Eignung nach den Artikeln 55–57 ISG beantragen, wenn sie:

a. über eine ausreichende gesetzliche Grundlage verfügen;

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

c. mit dem VBS eine Leistungsvereinbarung abgeschlossen haben.

2 Die Leistungsvereinbarung nach Absatz 1 Buchstabe c regelt insbesondere:

a. die Anzahl durchzuführender Beurteilungen;

b. welche Stellen bei den Kantonen den Antrag zur Durchführung solcher Beurteilungen stellen können;

c. die Finanzierung der Leistungen, einschliesslich die Modalitäten.

3 Die Höhe der Gebühren richtet sich nach Artikel 19 Absatz 2.

8. Abschnitt: Schlussbestimmungen

Art. 25 Aufhebung und Änderung anderer Erlasse

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

Art. 26 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. 27 Inkrafttreten

Diese Verordnung tritt am 1. Januar 2024 in Kraft.

… Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Alain Berset
Der Bundeskanzler: Walter Thurnherr

Anhang 1
(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. Datum des Beginns des Aufenthalts in der Schweiz
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 des Hauptauftrags
43. Auftraggeberin
44. Bezeichnung der Aufträge
45. Klassifizierung
46. Meldungsdatum
47. Gültigkeitsbeginn
48. Gültigkeitsende
49. Kurzbezeichnung der Branche
50. Branchencode zur wirtschaftlichen Tätigkeit der Firma (NOGA-Code)

Anhang 2
(Art. 25)

Aufhebung und Änderung anderer Erlasse

I

Die Geheimschutzverordnung vom 29. August 1990[11] wird aufgehoben.

II

Die nachstehenden Erlasse werden wie folgt geändert:

1. Nachrichtendienstverordnung vom 16. August 2017[12]

Anhang 3 einleitender Satz (betrifft nur den französischen Text) und 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:
    10.6. der Fachstelle Betriebssicherheit: zur Durchführung von Betriebssicherheitsverfahren;

2. Verordnung vom 24. Juni 2009[13] über internationale militärische Kontakte

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 …[14] über das Betriebssicherheitsverfahren.

11 AS **1990** 1774
12 SR **121.1**
13 SR **510.215**
14 SR **…**

3. Verordnung vom 16. Dezember 2009[15] über militärische und andere Informationssysteme im VBS

Art. 68 und Anhang 31

Aufgehoben

15 SR **510.911**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verordnung über die Personensicherheitsprüfungen (VPSP)

vom …

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 41*b* Absatz 2 AIG und 6*a* Absatz 2 AwG;

c. die Prüfungen der Vertrauenswürdigkeit nach den Artikeln 29*a* AsylG, 20*b* BPG, 14 MG und 20*a* 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 Missbrauchspotenzials nach Artikel 113 Absatz 4 Buchstabe d MG;

f. die Zuverlässigkeitskontrollen nach Artikel 24 Absatz 1 KEG.

2 Sie regelt zudem:

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

b. die Sicherheitsbescheinigung für Personen;

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, die eine Prüfung nach Absatz 1 erfordern;

b. die Zuordnung der sicherheitsempfindlichen Tätigkeiten zu den Prüfstufen;

c. die zuständigen einleitenden und entscheidenden Stellen.

Art. 2 Geltungsbereich

1 Diese Verordnung gilt für:

a. die verpflichteten Behörden nach Artikel 2 Absatz 1 ISG;

b. die Verwaltungseinheiten der zentralen Bundesverwaltung nach Artikel 7 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[9];

c. die Armee;

d. die Kantone.

2 Die Geltung dieser Verordnung für die Verwaltungseinheiten der dezentralen Bundesverwaltung nach Artikel 2 Absatz 3 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[10] (RVOG) und Organisationen nach Artikel 2 Absatz 4 RVOG richtet sich nach Artikel 2 Absätze 2 und 3 der Informationssicherheitsverordnung vom ...[11] (ISV).

3 Vorbehalten bleiben die eigenen Ausführungsbestimmungen nach Artikel 84 Absatz 1 ISG der verpflichteten Behörden über:

a. die Funktionen, für welche die Ausübung einer sicherheitsempfindlichen Tätigkeit erforderlich ist;

b. die Zuordnung der sicherheitsempfindlichen Tätigkeiten zu den Prüfstufen;

c. die zuständigen einleitenden und entscheidenden Stellen.

9 SR **172.010.1**
10 SR **172.010**
11 SR **...**

2. Abschnitt: Funktionenlisten

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

1 Für die Bundesverwaltung und Organisationen nach Artikel 2 Absatz 4 RVOG[12] 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.

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

4 Die Projektanten einer neuen Kernanlage, Inhaber einer Rahmen-, 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 Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) kann auf Antrag der Departemente und der Bundeskanzlei über die Ergänzung oder Änderung der Funktionenlisten nach den Anhängen 1–6 entscheiden. 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[13] nicht in der Amtlichen Sammlung veröffentlicht.

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

12 SR **172.010**
13 SR **170.512**

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 drei 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
(Art. 29 Abs. 3 ISG)

Das VBS entscheidet über ausserordentliche Prüfungen nach Artikel 29 Absatz 3 ISG. Es konsultiert vorgängig die Fachstelle des Bundes für Informationssicherheit.

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, ob eine Funktion von kantonalen Angestellten die Ausübung einer sicherheitsempfindlichen Tätigkeit beinhaltet. Es konsultiert vorgängig die Fachstelle des Bundes für Informationssicherheit. Vorbehalten bleibt Artikel 10 Absatz 2 Buchstabe e.

[2] Bevor bei Dritten eine Personensicherheitsprüfung durchgeführt wird, prüfen folgende Stellen, ob eine sicherheitsempfindliche Tätigkeit vorliegt:

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

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

Art. 9 Ausserordentliche Zuverlässigkeitskontrolle des ENSI

Funktionen, welche die Voraussetzungen nach Artikel 24 Absatz 1 KEG nur kurzzeitig erfüllen, werden nicht in den Funktionenlisten nach Artikel 3 Absatz 4 aufgeführt. Über die Zuverlässigkeit von Personen entscheidet das ENSI. 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: Zuordnung zu den Prüfstufen

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

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

a. die Bearbeitung als «vertraulich» klassifizierter Informationen;

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

c. der Zugang zu einer Sicherheitszone 1 nach Artikel 35 Absatz 1 Buchstabe a ISV[14] oder einer Schutzzone 2 nach Artikel 3 Absatz 2 Buchstabe b der Anlageschutzverordnung vom 2. Mai 1990[15];

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 als «geheim» klassifizierter Informationen;

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

c. der Zugang zu einer Sicherheitszone 2 nach Artikel 35 Absatz 1 Buchstabe b ISV oder einer Schutzzone 3 nach Artikel 3 Absatz 2 Buchstabe c der Anlageschutzverordnung;

d. sicherheitsempfindliche Tätigkeiten von Angestellten des Bundes und externen Mitarbeitenden:
   1. beim Nachrichtendienst des Bundes (NDB),
   2. beim militärischen Nachrichtendienst (MND),
   3. beim Dienst Cyber und elektromagnetische Aktionen (CEA),
   4. bei der unabhängigen Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten (AB-ND);

e. sicherheitsempfindliche Tätigkeiten von Mitarbeitenden der kantonalen Vollzugsbehörden nach Artikel 9 Absatz 1 des Nachrichtendienstgesetzes vom 25. September 2015[16] (NDG);

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

14 SR **…**
15 SR **510.518.1**
16 SR **121**

Art. 11 Prüfung der Vertrauenswürdigkeit nach dem BPG

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

a. hoheitliche Tätigkeiten nach Artikel 20*b* Absatz 1 Buchstabe a BPG von im Ausland eingesetzten Angestellten des Bundes und von versetzungspflichtigen Angestellten des Eidgenössischen Departements für auswärtige Angelegenheiten;

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 nach Artikel 20*b* Absatz 1 Buchstabe c BPG des Personals des Bundesamts für Polizei (fedpol), des Bundesamts für Justiz sowie des Bundesamts für Zoll und Grenzsicherheit, insbesondere in Bezug auf die operativen Mittel und Methoden zur Bekämpfung von Verbrechen oder Vergehen oder auf die Identität exponierter Personen;

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

a. Tätigkeiten im Rahmen von Arbeitsverhältnissen, für deren Begründung, Änderung und Beendigung nach Artikel 2 Absatz 1 der Bundespersonalverordnung vom 3. Juli 2001[17] (BPV) der Bundesrat 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 zuständig ist;

c. Tätigkeiten von Leiterinnen und Leitern von dezentralen 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 nach Artikel 20*b* Absatz 1 Buchstabe c BPG des Personals von fedpol, bei deren vorschriftswidriger oder unsachgemässer Ausübung die Bekämpfung von Schwerstkriminalität in Bundeskompetenz schwerwiegend gefährdet werden kann;

f. 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;

17 SR **172.220.111.3**

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 Absatz 3 Buchstabe d MG darf für Anwärterinnen und Anwärter nur verlangt werden, wenn:

a. für die neue Funktion ein Prüfgrund nach Absatz 1 oder nach Artikel 10 vorliegt; und

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

3 Einer Beurteilung des Gefährdungs- oder Missbrauchspotenzials nach Artikel 113 Absatz 4 Buchstabe d MG werden auf Antrag des Kommando Ausbildung unterzogen:

a. alle Stellungspflichtigen;

b. alle Angehörigen des Rotkreuzdienstes, die mit einer persönlichen Waffe ausgerüstet werden;

c. Angehörige der Armee, wenn ein Verdacht gemeldet wurde, dass:

1. sie sich selbst oder Dritte mit der persönlichen Waffe gefährden könnten, oder

2. sie oder Dritte die persönliche Waffe missbrauchen könnten.

4 Bei Stellungspflichtigen erfolgen die Prüfverfahren im Rahmen der Rekrutierung.

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 Zugang zu als «vertraulich» klassifizierten Informationen über Kernanlagen und Kernmaterialien haben;

b. Personen, die Tätigkeiten ausüben, welche bei ungetreuer Ausübung die Einhaltung der grundlegenden Schutzziele nach Artikel 1 Buchstabe d der Verordnung des UVEK vom 17. Juni 2009[18] über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen erheblich beeinträchtigen können;

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

2 Einer erweiterten Personensicherheitsprüfung sind die Zuverlässigkeitskontrollen von Personen zugeordnet, die Zugang zu als «geheim» klassifizierten Informationen über Kernanlagen und Kernmaterialien haben.

18 SR **732.112.2**

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 zu 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 zu 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 Wird gestützt auf Artikel 53 Absatz 2 ISG auf die Durchführung des Betriebssicherheitsverfahrens verzichtet, so ist die Auftraggeberin die einleitende und entscheidende Stelle.

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

a. einleitende Stellen: die Projektanten einer neuen Kernanlage, die Inhaber von Rahmen-, Bau- oder Betriebsbewilligungen oder die Adressaten von Stilllegungsverfügungen für Kernanlagen;

b. entscheidende Stelle: das ENSI.

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

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

7 Die einleitende Stelle ist für den Nachweis der Einwilligung zur Durchführung der Prüfungen zuständig, sofern das Informationssystem nach Artikel 45 ISG diesen nicht erbringt.

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 VBS (Fachstelle PSP VBS).

2 Die Fachstelle PSP VBS ist Teil des Staatssekretariats für Sicherheitspolitik im VBS.

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

a. Funktionen nach Artikel 2 Absatz 1 BPV[19], mit Ausnahme von Funktionen innerhalb der Bundeskanzlei;

b. Funktionen nach Artikel 2 Absatz 1bis BPV;

c. Funktionen innerhalb der Fachstelle PSP VBS;

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

4 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 die folgenden formellen Voraussetzungen erfüllt sind:

a. Die betreffende Funktion ist auf der Funktionenliste enthalten oder die Voraussetzungen nach den Artikel 7 oder 8 sind erfüllt.

b. Die Prüfung ist von der dafür zuständigen Stelle eingeleitet worden.

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

d. Alle Angaben der zu prüfenden Person, die für die Datenerhebung und die Verfahrensführung notwendig sind, liegen vor.

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

3 Ist eine Voraussetzung 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:

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 kann dies in die Risikobeurteilung miteinfliessen.

19 SR **172.220.111.3**

Art. 19 Datenerhebung
(Art. 27 und 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, bei:

a. Personen, die in einem Arbeitsverhältnis nach Artikel 2 Absatz 1 BPV[20] stehen;

b. Personen, die in einem Arbeitsverhältnis nach Artikel 2 Absatz 1bis BPV stehen;

c. Personen, die bei einer der folgenden Stellen eine Funktion ausüben oder dafür vorgesehen sind:
   1. NDB,
   2. kantonale Vollzugsbehörde nach Artikel 9 NDG[21],
   3. MND,
   4. CEA,
   5. AB-ND,
   6. fedpol,
   7. Fachstellen PSP;

d. Personen, die als Angestellte des Bundes als «geheim» klassifizierte Informationen bearbeiten müssen und:
   1. einen weitreichenden Einblick in wichtige sicherheitspolitische Geschäfte haben und darauf wesentlich Einfluss nehmen können, oder
   2. Aufsichts- oder Koordinationsaufgaben betreffend Funktionen nach Buchstabe c haben;

e. Personen, für die aufgrund eines völkerrechtlichen Vertrags eine Befragung vorgeschrieben ist.

3 Bei der Wiederholung von Personensicherheitsprüfungen können die Fachstellen PSP auf die Befragung verzichten, wenn die vorhandenen Daten für die Beurteilung des Sicherheitsrisikos ausreichend sind.

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, welche die zu prüfende Person betreuen oder betreut haben;

b. Bildungsinstitutionen, an denen die zu prüfende Person Ausbildungen 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.

20 SR **172.220.111.3**
21 SR **121**

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

Art. 20 Amtshilfe
(Art. 35 ISG)

1 Die 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 verschiedenen Prüfstufen zugeordnet, so wird das Prüfverfahren nach den Anforderungen der höheren Prüfstufe durchgeführt.

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. bei der zu prüfenden Person medizinische oder psychologische Abklärungen durchzuführen, insbesondere betreffend die Urteils- und Entscheidungsfähigkeit sowie den Konsum von Alkohol, Drogen, Betäubungsmitteln oder sonstigen Suchtmitteln;

c. Massnahmen nach Artikel 25 BPG zu treffen;

d. sofern es sich bei der zu prüfenden Person um eine Stellungspflichtige oder einen Stellungspflichtigen beziehungsweise eine Angehörige oder einen An-

gehörigen der Armee handelt: Massnahmen betreffend den Besitz der persönlichen Waffe zu ergreifen;

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 verschiedenen Prüfgründen und stellt eine Fachstelle PSP bei einer späteren Prüfung ein Sicherheitsrisiko fest, so teilt sie ihre Erklärung den für die früheren Prüfungen entscheidenden Stellen mit. Vorbehalten bleibt Artikel 25 Absatz 2.

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. ernstzunehmende Anzeichen oder Hinweise nach Artikel 113 Absatz 1 MG;

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

c. 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 Mittelung des Entscheids über die Ausübung der Tätigkeit
(Art. 41 ISG)

1 Die entscheidende Stelle teilt ihren Entscheid über die Ausübung der Tätigkeit (Art. 41 Abs. 2 ISG) der geprüften Person und der zuständigen Fachstelle PSP innerhalb von einem Monat mit.

2 Bei einer Sicherheitserklärung nach Artikel 39 Absatz 1 Buchstabe a ISG wird die Zulassung zur Ausübung der Tätigkeit vermutet. Die entscheidende Stelle kann auf die Mitteilung verzichten.

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 Die ordentliche Wiederholung einer Prüfung ist einzuleiten:

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

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

2 Vorbehalten bleiben Fristen aufgrund eines völkerrechtlichen Vertrags.

3 Bei Funktionen der Armee und des Zivilschutzes wird die Grundsicherheitsprüfung nicht ordentlich wiederholt, wenn die zu prüfende Person die Funktion voraussichtlich noch weniger als fünf Jahre ausüben soll.

4 Beurteilungen des Gefährdungs- oder Missbrauchspotenzials nach Artikel 113 Absatz 4 Buchstabe d MG werden nicht ordentlich wiederholt.

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)

Bis zum neuen Entscheid nach Artikel 41 Absatz 1 ISG bleibt der bisherige Entscheid gültig.

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
(Art. 48 Bst. c ISG)

[1] Für die Ausstellung von Sicherheitsbescheinigungen im nationalen und 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 der Daten, die ausserhalb des Informationssystems nach Artikel 45 Absatz 5 ISG bearbeitet werden, ist die bearbeitende Stelle verantwortlich.

[3] Die Daten dürfen ausschliesslich zur Personensicherheitsprüfung verwendet werden.

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: Vollzugsbestimmungen

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

[1] Der Geschäftsverkehr zwischen der zu prüfenden Person, den Behörden, Drittpersonen und Gerichtsinstanzen erfolgt elektronisch.

[2] Personen, die nicht beim Bund angestellt sind, können verlangen, dass der Geschäftsverkehr mit ihnen in Papierform erfolgt.

3 Die Fachstellen PSP können zugelassene Zustellplattformen und Identitätsverzeichnisse verwenden.

Art. 34 Gebührenerhebung

1 Für die Durchführung von Prüfungen bei Stellen ausserhalb der zentralen Bundesverwaltung und der Armee 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 Für die PSP nach dem ISG und die Prüfungen der Vertrauenswürdigkeit nach Artikel 20*b* BPG werden keine Gebühren erhoben.

4 Im Übrigen gilt die Allgemeine Gebührenverordnung vom 8. September 2004[22] (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 Die Leistungsvereinbarung nach Absatz 1 Buchstabe c regelt insbesondere:

a. die Anzahl durchzuführender Prüfungen;

b. die einleitenden und entscheidenden Stellen beim Kanton;

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[23].

9. Abschnitt: Schlussbestimmungen

Art. 36 Aufhebung und Änderung anderer Erlasse

Die Aufhebung und die Änderung anderer Erlasse werden in Anhang 8 geregelt.

22 SR **172.041.1**
23 SR **172.041.1**

Art. 37 Übergangsbestimmungen

[1] Das ISG und diese Verordnung sind auf Beurteilungen anwendbar, die im Zeitpunkt des Inkrafttretens dieser Verordnung hängig sind. Die Fachstellen PSP prüfen in Zusammenarbeit mit den einleitenden Stellen, ob die Voraussetzungen für die Durchführung der Prüfungen weiterhin erfüllt sind.

[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] Für Personen in Funktionen, für die nach neuem Recht eine erstmalige Prüfung oder eine Prüfung in einer höheren Prüfstufe durchgeführt werden muss, ist innert sechs Monaten die erforderliche Prüfung einzuleiten. Die entscheidende Stelle legt fest, ob die Person die sicherheitsempfindlichen Tätigkeiten bis zum Entscheid nach Artikel 41 Absatz 2 ISG weiterhin ausüben darf. Ergeben sich während der Prüfung Anzeichen auf Sicherheitsrisiken, so trifft die entscheidende Stelle die notwendigen vorsorglichen Massnahmen.

[4] Sicherheitsprüfungen, die die nationale Netzgesellschaft vor und bis ein Jahr nach Inkrafttreten dieser Verordnung 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 höchstkritische Funktionen: als erweiterte Personensicherheitsprüfung nach dieser Verordnung.

Art. 38 Inkrafttreten

Diese Verordnung tritt am 1. Januar 2024 in Kraft.

… Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Alain Berset
Der Bundeskanzler: Walter Thurnherr

Anhang 1[24]
(Art. 3 Abs. 1 Bst. a)

Funktionen der Bundesverwaltung, die einer Personensicherheitsprüfung nach ISG unterstehen

Wird nicht veröffentlicht

24 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

Verwaltungseinheit	Funktion	Grundsicherheitsprüfung
SEM, DB AS/Abt. Analysen und Services	Dolmetscherinnen und Dolmetscher	x
SEM, DB AS/Abt. Analysen und Services	Übersetzerinnen und Übersetzer	x

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	Grundsicherheitsprüfung (Art. 11 Abs. 1 VPSP)		
		Bst. a	Bst. b	Bst. c
1. Bundeskanzlei				
keine				
2. EDA				
Staatssekretariat, Auslandsvertretungen	Karriere Diplomatie	x		
	Karriere KBF	x		
	Karriere Internationale Zusammenarbeit	x		
	Fachpersonal versetzbar	x		
3. EDI				
keine				

Verwaltungseinheit	Funktion	Grundsicherheitsprüfung (Art. 11 Abs. 1 VPSP)		
		Bst. a	Bst. b	Bst. c
4. EJPD				
BJ, Auslieferung	Co-Chef/in AUSL			x
	FV internationale Personenfahndungen			x
	Jurist/in			x
	Sachbearbeiter/in			x
	Sekretär/in			x
	Stv. Chef/in AUSL			x
BJ, DB internationale Rechtshilfe	Chef/in IRH, Vizedirektorin			x
	Direktionsbereichsassistent/in			x
	Verbindungsstaatsanwalt/-anwältin Eurojust			x
BJ, Internationale Verträge	Chef/in INTV			x
	Jurist/in			x
	Stv. Chef/in INTV			x
BJ, Rechtshilfe I	Chef/in RH I			x
	Stv. Chef/in RH I			x
	Expert/in Wirtschaft und Finanzen			x

Verwaltungseinheit	Funktion	Grundsicherheitsprüfung (Art. 11 Abs. 1 VPSP)		
		Bst. a	Bst. b	Bst. c
	Jurist/in			x
	Sachbearbeiter/in, Assistent/in			x
BJ, Rechtshilfe II	Chef/in RH II, Stv. Chef/in IRH			x
	Stv. Chef/in RH II			x
	Fachverantwortliche/r Rechtshilfeersuchen			x
	Jurist/in			x
	Sekretär/in			x
BJ, Internationaler Menschenrechtsschutz	Chef/in IMRS / Agent du Gouvernement	x		
BJ, Trova Services (TS)	Aushilfe			x
	Fachspezialist/in TROVA I			x
	Fachspezialist/in TROVA II			x
	Leiter/in TS			x
	Sachbearbeiter/in			x
	Stv. Leiter/in TS/Fachspezialist/in TRIVA II			x
BJ, Infostar	Chef/in FIS			x
	Sachbearbeiter/in II			x

Verwaltungseinheit	Funktion	Grundsicherheitsprüfung (Art. 11 Abs. 1 VPSP)		
		Bst. a	Bst. b	Bst. c
	Stv. Leiter/in FIS, Anforderungsmanager			x
BJ, Strafregister	Chef/in SSR			x
	Stv. Chef/in SSR			x
	Jurist/in			x
	Sachbearbeiter/in I VOSTRA			x
	Sachbearbeiter/in II VOSTRA			x
	Sekretär/in			x
	Spezialist/in I VOSTRA			x
	Spezialist/in II VOSTRA			x
BJ, Rechtsinformatik	Anwendungsverantwortlich/r VOSTRA			x
	Anwendungsverantwortlich/r VOSTRA Schnittstellen			x
5. VBS				
keine				

Verwaltungseinheit	Funktion	Grundsicherheitsprüfung (Art. 11 Abs. 1 VPSP)		
		Bst. a	Bst. b	Bst. c
6. EFD				
EFV, Bundestresorerie	Mitarbeitende Frontoffice Tresorerie		x	
	Mitarbeitende Backoffice Tresorerie		x	
	Mitarbeitende Sparkasse Bundespersonal		x	
EFV, Finanz- und Rechnungswesen Bund	Leiter/in Zentrales Rechnungswesen		x	
	Mitarbeitende Zahlungsmanagement		x	
EFV, Swissmint	Geschäftsleiter/in		x	
	Leiter/in Managementsysteme		x	
	Leiter/in Marketing/Verkauf		x	
	Fachspezialist/in Administration / Marketing		x	
	Fachspezialist/in Münzdesign / Gravieratelier		x	
	Leiter/in Technik		x	
	Fachspezialist/in Werkzeugherstellung		x	
	Fachspezialist Produktion		x	
EPA, Finanzdienst	Leiter/in Finanzdienst		x	

Verwaltungseinheit	Funktion	Grundsicherheitsprüfung (Art. 11 Abs. 1 VPSP)		
		Bst. a	Bst. b	Bst. c
BAZG, P+S,	Chef/in Planung & Steuerung			x
BAZG, P+S, Programme/ DaziT/Informatik	Chef/in ICT COO			x
BAZG, P+S, Unternehmensentwicklung und Portfoliomanagement	Chef/in Unternehmensentwicklung und Portfoliomanagement, CIO			x
	Datenschutzbeauftragte/r BAZG			x
	Informationssicherheitsbeauftragte/r BAZG (ISBO)			x
BAZG. Grundlagen	Chef/in Grundlagen			x
BAZG, Grundlagen, Führungsunterstützung	Chef/in Führungsunterstützung			x
BAZG, Grundlagen, Grenzsicherheit	Chef/in Grenzsicherheit			x
	Chef/in Personensicherheit & nat. Sicherheitszusammenarbeit			x
	Fachspezialist/in Personensicherheit & nat. Sicherheitszusammenarbeit			x
	Chef/in Grenzkontrollsysteme			x
	Fachspezialist/in Grenzkontrollsysteme			x

Verwaltungseinheit	Funktion	Grundsicherheitsprüfung (Art. 11 Abs. 1 VPSP)		
		Bst. a	Bst. b	Bst. c
	Chef/in Warensicherheit			x
	Experte/Expertin Frontex Attaché	x		x
BAZG, Risikoanalyse und Analytik, Business Intelligence/ Analytics	Chef/in Business Intelligence & Analytics			x
BAZG, Risikoanalyse und Analytik, Datenservice	Chef/in Datenservices			x
BAZG, Risikoanalyse und Analytik, Information und Lage	Chef/in Information und Lage und Stv.			x
	Chef/in Informationsmanagement			x
	Fachexperte/-expertin Informationsmanagement			x
	Chef/in Lage und Stv.			x
	Fachexperte/-expertin Lage			x
	Chef/in Nachrichtennetzwerk			x
	Attaché/e BAZG	x		x
	Verbindungsoffizier/in fedpol			x
	Verbindungsoffizier/in Nachrichtennetzwerk			x
	Verbindungsoffizier/in NDB			x

Verwaltungseinheit	Funktion	Grundsicherheitsprüfung (Art. 11 Abs. 1 VPSP)		
		Bst. a	Bst. b	Bst. c
BAZG, Risikoanalyse und Analytik, Risikoanalyse	Chef/in Risikoanalyse und Analytik			x
	Chef/in Risikoanalyse			x
	Chef/in Money			x
	Fachexperte/-expertin Money			x
	Chef/in Security			x
	Fachexperte/-expertin Security			x
	Chef/in Safety			x
	Fachexperte/-expertin Safety			x
	Chef/in Risikoanalyse Regionalebene			x
	Fachspezialist/in Risikoanalyse Regionalebene			x
	Fachspezialist/in Risikoanalyse Regionalebene und Stv.			x
BAZG, StV	Chef/in Strafverfolgung			x
BAZG, StV, INVE	Chef/in Informationsgewinnung und Vorermittlung			x
	Fachexperte/-expertin Zoll- und Polizeikooperation			x
	Verbindungsattaché/e BAZG (Europol)	x		x
	Chef/in Informationsgewinnung			x

Verwaltungseinheit	Funktion	Grundsicherheitsprüfung (Art. 11 Abs. 1 VPSP)		
		Bst. a	Bst. b	Bst. c
	Inspektor/in Digitalforensik			x
	Inspektor/in OSINT und Netzwerkanalyse			x
	Chef/in Vorermittlung			x
	Chef/in Vorermittlung und Stv.			x
	Inspektor/in Vorermittlung			x
BAZG, StV, MEK	Chef/in Mobiles Einsatzkommando (MEK) Helvetia			x
	Stv. Chef/in MEK			x
	Chef/in Einsatzkoordination MEK			x
	Chef/in Gruppe MEK			x
	Equipenchef/in MEK			x
	Fachspezialist/in Observation MEK			x
	Chef/in Gruppe Technik MEK			x
	Fachspezialist/in Technik MEK			x
BAZG, StV, Zollfahndung	Chef/in Zollfahndung			x
	Chef/in Zollfahndung und Stv.			x
	Assistent/in Zollfahndung			x
	Chef/in Untersuchungsgruppe Zollfahndung			x

Verwaltungseinheit	Funktion	Grundsicherheitsprüfung (Art. 11 Abs. 1 VPSP)		
		Bst. a	Bst. b	Bst. c
	Chef/in Untersuchungsgruppe Zollfahndung und Stv.			x
	Inspektor/in Zollfahndung			x
BAZG, USTÜ	Chef/in Unterstützung			x
BAZG, OP, Ebene Direktion	Chef/in Operationen			x
	Chef/in Stab Operationen			x
	Koordinator/in Tiger/ Fox Operationen			x
BAZG, OP, Regionalebene	Chef/in Regionalebene RE			x
BAZG, OP, Lokalebene	Chef/in Lokalebene			x
PUBLICA, Buchhaltung	Fachspezialist/in Buchhaltung		x	
	Stv. Leiter/in Buchhaltung		x	
PUBLICA, Immobilien	Leiter/in Immobilien		x	
	Stv. Leiter/in Immobilien		x	
	Portfolio Manager		x	
PUBLICA, Portfolio Management	Portfolio Manager		x	
	Senior Portfolio Manager		x	

Verwaltungseinheit	Funktion	Grundsicherheitsprüfung (Art. 11 Abs. 1 VPSP)		
		Bst. a	Bst. b	Bst. c
PUBLICA, Private Markets	Private Markets Spezialist		x	
PUBLICA, Operations, Risk & Compliance	Sachbearbeiter/in ORC		x	
	Stv. Leiter/in ORC		x	
PUBLICA, Asset Management	Leiter/in Asset Management		x	
7. WBF				
SBFI	Detachierte	x		
SBFI, Abteilung Raumfahrt	Leiter/in		x	
	Gruppenleiter/in		x	
	Wissenschaftliche/r Berater/in, Programmverantwortliche/r		x	
8. UVEK				
keine				

2. in der Prüfstufe «erweiterte Personensicherheitsprüfung»:

Verwaltungseinheit	Funktion	Erweiterte Personensicherheitsprüfung (Art. 11 Abs. 2 VPSP)						Befragung (Art. 19 Abs. 2)
		Bst. a	Bst. b	Bst. c	Bst. d	Bst. e	Bst. f	
1. Bundeskanzlei								
BK, Fachstelle PSP	Leiter/in Fachstelle PSP BK						x	x
BK, Fachstelle PSP	Risk Profiler/in						x	x
BK, Bereich DTI	Delegierte/r des Bundesrats für digitale Transformation und IKT-Lenkung	x						x
BK, Bereich Bundesrat	Vizekanzler/in	x						x
BK, Bereich Kommunikation und Strategie	Vizekanzler/in	x						x
2. EDA								
Allgemein	Generalsekretär/in, Staatssekretär/in und Amtsdirektor/in	x						x
	Stv. Generalsekretär/in, Stv. Staatssekretär/in und Stv. Amtsdirektor/in		x					x
	Missionschef/in	x						x

Verwaltungseinheit	Funktion	Erweiterte Personensicherheitsprüfung (Art. 11 Abs. 2 VPSP)						Befragung (Art. 19 Abs. 2)
3. EDI								
Allgemein	Generalsekretär/in und Amtsdirektor/in	x						x
	Stv. Generalsekretär/in und Stv. Amtsdirektor/in		x					x
4. EJPD								
Allgemein	Generalsekretär/in, Staatssekretär/in und Amtsdirektor/in	x						x
	Stv. Generalsekretär/in, Stv. Staatssekretär/in und Stv. Amtsdirektor/in		x					x
Dienst ÜPF	Direktor/in			x				
SIR	Direktor/in			x				
IGE	Direktor/in			x				
RAB	Direktor/in			x				
METAS	Direktor/in			x				

Verwaltungseinheit	Funktion	Erweiterte Personensicherheitsprüfung (Art. 11 Abs. 2 VPSP)						Befragung (Art. 19 Abs. 2)
5. VBS								
Allgemein	Generalsekretär/in, Staatssekretär/in und Amtsdirektor/in	x						x
	Stv. Generalsekretär/in, Stv. Staatssekretär/in und Stv. Amtsdirektor/in		x					x
SEPOS	Personal der Fachstelle PSP VBS						x	x
	Chef/in Steuerung und Koordination	x						x
Gruppe V, Armeestab (A Stab)	CdA	x						x
	Chef A Stab	x						x
	SC CdA	x						x
	SCOS	x						x
	C Armeeplanung / Stv C A Stab	x	x					x
	ZHSO CdA	x						x
	Projektleiter Kommando Cyber	x						x
	HSO Genfer Zentrum für Sicherheitspolitik	x						x
	MA Spez Einsätze / MIL Ber C VBS	x						x
	Sen Mil Representative to NATO	x						x
	Chef Internationale Beziehungen V	x						x

Verwaltungseinheit	Funktion	Erweiterte Personensicherheitsprüfung (Art. 11 Abs. 2 VPSP)						Befragung (Art. 19 Abs. 2)
	VA (HSO)	x						x
Gruppe V, Kommando Operationen (Kdo Op)	Chef Kdo Op	x						x
	Stv. Chef Kdo Op	x	x					x
	Stabschef Kdo Op	x						x
	Chef MND & DPSA	x						x
	Kdt Heer	x						x
	Kdt Mechanisierte Brigade 1	x						x
	Kdt Mechanisierte Brigade 4	x						x
	Kdt Mechanisierte Brigade 11	x						x
	Kdt Ter Div 1	x						x
	Stv Kdt Ter Div 1 / Kdt PdG	x						x
	SC HQ / Chef Ausb Ter Div 1	x						x
	Kdt Koord Stelle 1	x						x
	Kdt Ter Div 2	x						x
	Stv. Kdt Ter Div 2	x						x
	Kdt Ter Div 3	x						x
	Stv. Kdt Ter Div 3	x						x
	Kdt Ter Div 4	x						x

Verwaltungseinheit	Funktion	Erweiterte Personensicherheitsprüfung (Art. 11 Abs. 2 VPSP)						Befragung (Art. 19 Abs. 2)
	Stv. Kdt Ter Div 4	x						x
	Kdt LW	x						x
	Kdt Stv LW	x						x
	Kdt BODLUV Br 33	x						x
	Kdt Militärpolizei	x						x
	Chief of Staff	x						x
	Delegationsleiter	x						x
Gruppe V, Logistikbasis der Armee (LBA)	Chef/in LBA	x						x
	Stv. C LBA	x	x					x
	Chef Sanität / Oberfeldarzt	x						x
Gruppe V, Kommando Cyber (Kdo Cy)	C Kdo Cy	x						x
	Kdt FU Br 41	x						x
Gruppe V, Kommando Ausbildung (Kdo Ausb)	Kdt Generalstabsschule	x						x
	Kdt HKA / Stv C Ausbildung	x	x					x
	Kdt Militärakademie	x						x
	Kdt Zentralschule	x						x
	Kdt Lehrverband Genie/Rettung/ABC	x						x

Verwaltungseinheit	Funktion	Erweiterte Personensicherheitsprüfung (Art. 11 Abs. 2 VPSP)						Befragung (Art. 19 Abs. 2)
	Kdt Lehrverband Logistik	x						x
	Kdt Lehrverband Panzer/Artillerie	x						x
	Chef Personelles der Armee	x						x
	Chef Kdo Ausbildung / Stv CdA	x	x					x
AB-ND	Leiter/in der AB-ND			x				x
6. EFD								
Allgemein	Generalsekretär/in, Staatssekretär/in und Amtsdirektor/in	x						x
	Stv. Generalsekretär/in, Stv. Staatssekretär/in und Stv. Amtsdirektor/in		x					x
EPA, Personalwirtschaft	Leiter Pers Wirtschaft und Budgetierung				x			
EFK	Direktor/in			x				
PUBLICA	Direktor/in			x				
7. WBF								
Allgemein	Generalsekretär/in, Staatssekretär/in und Amtsdirektor/in	x						x

Verwaltungseinheit	Funktion	Erweiterte Personensicherheitsprüfung (Art. 11 Abs. 2 VPSP)						Befragung (Art. 10 Abs. 2)
	Stv. Generalsekretär/in, Stv. Staatssekretär/in und Stv. Amtsdirektor/in		x					x
BLW	Ständig für das BLW im Ausland tätige Personen				x			
SECO, Direktion für Standortförderung	Leiter/in	x						x
ETH-Bereich, ETH-Rat	Präsident/in			x				
ETH-Bereich, ETH Zürich	Präsident/in			x				
ETH-Bereich, EPFL	Präsident/in			x				
ETH-Bereich, PSI	Direktor/in			x				
ETH-Bereich, EMPA	Direktor/in			x				
ETH-Bereich, WSL	Direktor/in			x				
ETH-Bereich, Eawag	Direktor/in			x				
8. UVEK								
Allgemein	Generalsekretär/in, Staatssekretär/in und Amtsdirektor/in	x						x
	Stv. Generalsekretär/in, Stv. Staatssekretär/in und Stv. Amtsdirektor/in		x					x

Anhang 4[25]
(Art. 3 Abs. 2 Bst. a)

Funktionen der Armee, die einer Personensicherheitsprüfung nach dem ISG unterstehen

Wird nicht veröffentlicht

25 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»:

Organisation	**Funktion**	**Grundsicherheitsprüfung (Art. 12 Abs. 1 Bst. a und b VPSP)**	
		Bst. a	**Bst. b**
A Stab	VA in Ausbildung (ausser HSO)	x	
	Verteidigungsattaché & Stv.	x	

Anhang 6[26]
(Art. 3 Abs. 3)

Funktionen nach Artikel 20*a* Absatz 1 StromVG

Wird nicht veröffentlicht

26 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 erhoben und 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. Biologisches Geschlecht und Geschlechtsidentität,
   6. Telefonnummern (Festnetz und Mobilnetz),
   7. E-Mail-Adressen (beruflich und privat),
   8. AHV-Nummer bzw. bei Ausländern entsprechende Identifikationsnummern,
   9. ID- und Passangaben,
   10. Nationalitäten,
   11. Ein- und Ausbürgerungen,
   12. Heimatort,
   13. Geburtsort,
   14. Social Media Accounts / Mitgliedschaften;

b. Daten über die Lebensführung der zu prüfenden Person, insbesondere:
   1. schulischer Werdegang,
   2. Ausbildungen,
   3. beruflicher Werdegang und Tätigkeiten inklusive Personaldossier,
   4. Nebenbeschäftigungen,
   5. Werdegang innerhalb der Armee, des Zivilschutzes oder des Zivildienstes,
   6. Hobbies und Freizeitaktivitäten,
   7. ehrenamtliche Tätigkeiten,
   8. religiöse Ansichten oder Tätigkeiten,
   9. weltanschauliche Ansichten,
   10. politische Ansichten oder Tätigkeiten,
   11. gewerkschaftliche Ansichten oder Tätigkeiten,
   12. Dauer des Aufenthaltes in der Schweiz oder in Drittstaaten,
   13. frühere Wohnorte und Adressen;

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. Auslandsaufenthalte,
   2. Geschäftsbeziehungen,
   3. personelle Beziehungen und internationale Kontakte,
   4. finanzielle Verflechtungen im Ausland;

e. Daten über die Gesundheit der zu prüfenden Person, insbesondere:
   1. physische und psychische Krankheiten / Beeinträchtigungen,
   2. Konsum von Betäubungsmittel und Alkohol bzw. bewusstseinsverändernden Substanzen aller Art,
   3. Süchte und Abhängigkeiten,
   4. Medikamente;

f. Finanzdaten der zu prüfenden Person, insbesondere:
   1. Einkommen und Vermögen,
   2. Unterstützungsleistungen,
   3. Hypotheken und Kredite,
   4. Schulden,
   5. Finanzanlagen und Investitionen;

g. Daten über zivil- und verwaltungsrechtliche, administrative, jugendstrafrechtliche oder strafrechtliche Verfahren und Sanktionen mit Beteiligung der zu prüfenden Person, insbesondere:
   1. Betreibungen und Konkurse,
   2. Strafuntersuchungen,
   3. Strafurteile,
   4. Vollzugsdaten,
   5. administrative Untersuchungen,
   6. Klagen und rechtliche Prozesse,
   7. Mediation,
   8. Rayonverbote,
   9. Waffen- und Ausweisentzüge,
   10. Einziehungen und Beschlagnahmungen;

h. Angaben über bisherige Risikofaktoren im Rahmen einer sicherheitsempfindlichen Tätigkeit der zu prüfenden Person;

i. Daten über Dritte / Bezugspersonen der zu prüfenden Person, insbesondere:
   1. Angaben nach den Buchstaben a–g über den Ehepartnerin oder die Ehepartner oder die Partnerin oder den Partner, bzw. den Familienkreis, bzw. den engen Freundeskreis, sofern diese Angaben gemäss Artikel 34 Absatz 3 ISG für die Beurteilung des Sicherheitsrisikos unerlässlich sind,
   2. Auftraggeber oder Auftraggeberin und dessen oder deren Adresse,
   3. Arbeitgeber und Geschäftspartner oder Geschäftspartnerinnen;

j. Daten durch mündlich und/oder schriftliche Befragung der zu prüfenden Person, wenn:
   1. sich gestützt auf die erhobenen Daten konkrete Hinweise auf ein Sicherheitsrisiko ergeben, oder
   2. für die Beurteilung nicht genügend Daten über einen hinreichenden Zeitraum vorhanden sind;

k. Daten aus den folgenden Quellen:
   1. aus dem Strafregister: sämtliche Daten,
   2. von den zivilen und militärischen Straf- und Massnahmenvollzugsbehörden: sämtliche Daten,
   3. von Organen des Bundes aus den folgenden Systemen und Registern:
      – Daten der Waffeninformationsplattform ARMADA
      – Daten des Informationssystems HOOGAN
      – Daten des Informationssystems NES
      – 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. von Sicherheitsorganen des Bundes, dem NDB, den Organen der Armee: sämtliche Daten,
   5. von weiteren Organen des Bundes: sämtliche Daten, die für die Beurteilung des Sicherheitsrisikos erforderlich sind,
   6. aus den Registern und Akten der Sicherheitsorgane der Kantone sowie der Polizei: sämtliche Daten,

7. aus den Registern der Betreibungs- und Konkursbehörden: sämtliche Daten,
8. aus den Akten bisheriger Prüfungen: sämtliche Daten, die nicht älter als zehn Jahre sind und noch nicht nach Artikel 47 ISG archiviert oder vernichtet sind,
9. aus öffentlich zugänglichen Quellen, insbesondere:
   - im Internet: Daten, die jeder Internet-Benutzerin oder jedem Internet-Benutzer nach der Errichtung eines Kontos, dem Bezahlen einer Gebühr oder dem Abschluss eines Abonnements zugänglich sind
   - in sozialen Medien: Daten, die jeder Benutzerin oder jedem Benutzer ohne persönliche Kontaktaufnahme zu einer anderen Benutzerin oder einem anderen Benutzer zugänglich sind
   - in nicht elektronischen Medien: Daten, die jeder Benutzerin oder jedem Benutzer mit oder ohne Nutzerabonnement und Gebühr zugänglich sind.

2. Daten, die bei der Prüfstufe «erweiterte Personensicherheitsprüfung» zusätzlich erhoben und 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 mündliche oder schriftliche Befragung der zu prüfenden Person: sämtliche Daten.

Anhang 8
(Art. 36)

Aufhebung und Änderung anderer Erlasse

I

Die folgenden Erlasse werden aufgehoben:

1. die Verordnung vom 4. März 2011[27] über die Personensicherheitsprüfungen;
2. die Verordnung der Bundeskanzlei vom 30. November 2011[28] über die Personensicherheitsprüfungen;
3. die Verordnung des WBF vom 2. November 2011[29] über die Personensicherheitsprüfungen;
4. die Verordnung des VBS vom 12. März 2012[30] über die Personensicherheitsprüfungen;
5. die Verordnung des EDA vom 14. August 2012[31] über die Personensicherheitsprüfungen;
6. die Verordnung des UVEK vom 15. Februar 2013[32] über die Personensicherheitsprüfungen;
7. die Verordnung des EJPD vom 26. Juni 2013[33] über die Personensicherheitsprüfungen;
8. die Verordnung des EDI vom 12. August 2013[34] über die Personensicherheitsprüfungen;
9. die Verordnung vom 9. Juni 2006[35] über die Personensicherheitsprüfungen im Bereich Kernanlagen.

II

Die nachstehenden Erlasse werden wie folgt geändert:

27 AS **2011** 1031**,** 5903; **2012** 1153, 3631, 3765, 5527, 6669; **2013** 3041; **2014** 4567; **2016** 1785; **2017** 4151, 4231; **2020** 5893; **2021** 589; **2022** 568, 689; **2023** 133
28 AS **2011** 6077; **2022** 118
29 AS **2011** 4999; **2013** 1335
30 AS **2012** 1161, 1597
31 AS **2012** 4241
32 AS **2013** 765
33 AS **2013** 2633
34 AS **2013** 2675
35 AS **2006** 2481; **2008** 5747; **2011** 1031

1. Verordnung vom 4. Dezember 2009[36] über verwaltungspolizeiliche Massnahmen des Bundesamtes für Polizei und über das Informationssystem HOOGAN

Art. 9 Abs. 1 Bst. f und 3 Bst. c

[1] Auf HOOGAN haben die folgenden Behörden ausschliesslich zu den folgenden Zwecken Zugriff:

f. die Fachstellen für Personensicherheitsprüfungen (Fachstellen PSP) nach Artikel 31 Absatz 2 des Informationssicherheitsgesetzes vom 18. Dezember 2020[37] zur Durchführung der Verfahren nach Artikel 1 Absatz 1 der Verordnung vom … [38] über die Personensicherheitsprüfungen.

[3] Über den Vollzugriff verfügen:

c. die Fachstellen PSP.

Anhang, Zeile Dienststelle, dritte Zelle

BAZG, Kantone, Fachstellen PSP

2. Bundespersonalverordnung vom 3. Juli 2001[39]

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

[1] Der Arbeitgeber kann von Bewerberinnen und Bewerbern sowie von Angestellten alle fünf Jahre oder aus wichtigen Gründen jederzeit einen Auszug aus dem Strafregister oder Betreibungsregister verlangen.

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

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

[1] Eine Prüfung der Vertrauenswürdigkeit von Bewerberinnen und Bewerbern sowie Angestellten kann unter den Voraussetzungen nach Artikel 11 der Verordnung vom …[40] über die Personensicherheitsprüfungen (VPSP) durchgeführt werden.

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

36 SR **120.52**
37 SR **128**
38 SR **…**
39 SR **172.220.111.3**
40 SR **…**

3. NES-Verordnung vom 15. Oktober 2008[41]

Art. 19 Abs. 1 Bst. i und 2 Einleitungssatz (Betrifft nur den französischen Text) und Bst. h

1 Die BKP kann, soweit dies zur Erlangung der von ihr benötigten Auskünfte und zur Begründung ihrer Amtshilfeersuchen nötig ist, im NES gespeicherte Personendaten folgenden weiteren Empfängern bekannt geben:

i. Bundesbehörden, die betraut sind mit:
   1. Personensicherheitsüberprüfungen nach den Artikeln 27–48 des Informationssicherheitsgesetzes (ISG) vom 18. Dezember 2020[42],
   2. Schutzmassnahmen im Sinne von Artikel 2 Absatz 2 Buchstabe b BWIS[43];

2 Darüber hinaus kann die BKP im NES gespeicherte Personendaten folgenden Behörden auf Anfrage bekannt geben, soweit die Daten zur Erfüllung der gesetzlichen Aufgabe der anfragenden Behörde erforderlich sind:

h. Bundesbehörden, die mit Personensicherheitsüberprüfungen nach den Artikeln 27–48 ISG oder Schutzmassnahmen im Sinne von Artikel 2 Absatz 2 Buchstabe b BWIS betraut sind;

4. Verordnung vom 24. Juni 2009[44] 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 …[45] über die Personensicherheitsprüfungen;

5. Verordnung vom 16. Dezember 2009[46] über militärische und andere Informationssysteme im VBS

Art. 67

Aufgehoben

41 SR **360.2**
42 SR **128**
43 SR 120
44 SR **510.215**
45 SR **…**
46 SR **510.911**

Art. 70s Bst. e

Die Daten des MIL PLATTFORM werden beschafft:

e. aus dem Informationssystem zur Personensicherheitsprüfung nach Artikel 45 Absatz 1 des Informationssicherheitsgesetzes vom 18. Dezember 2020[47] (ISG): die Daten nach Anhang 33*d* Ziffer 2.

Anh. 23a Ziff. 36

36. Prüfstufe nach Artikel 30 ISG[48], Datum der Rechtskraft des Entscheids nach Artikel 41 Absatz 2 ISG sowie Zeitpunkt der nächsten ordentlichen Wiederholung der Personensicherheitsprüfung nach Artikel 26 der Verordnung vom ...[49] über die Personensicherheitsprüfungen;

Anh. 30

Aufgehoben

Anh. 33d Ziff. 2

2. Prüfstufe nach den Artikeln 10–14 VPSP[50], Datum der Rechtskraft des Entscheids nach Artikel 24 VPSP sowie Zeitpunkt der nächsten ordentlichen Wiederholung der Personensicherheitsprüfung nach Artikel 26 VPSP betreffend einer zugangsberechtigten Person.

6. Verordnung vom 22. November 2017[51] über die Militärdienstpflicht

Art. 11 Abs. 3 Bst. g

3 An der Orientierungsveranstaltung werden die Teilnehmenden insbesondere informiert über:

g. die Personensicherheitsprüfung nach der Verordnung vom …[52] 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:

47 SR **128**
48 SR **128**
49 SR **...**
50 SR **...**
51 SR **512.21**
52 SR **…**

b. eine Personensicherheitsprüfung erforderlich ist, aber noch kein Entscheid nach Artikel 24 VPSP[53] 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 Fachoffiziere und Fachoffizierinnen, Spezialisten und Spezialistinnen, höhere Unteroffiziere und Offiziere für die Verlängerung der Militärdienstpflicht zugelassen werden, wenn:

b. die betroffene Person die folgenden Voraussetzungen erfüllt:

3. Die entscheidende Stelle lässt nach Artikel 41 Absatz 2 des Informationssicherheitsgesetzes vom 18. Dezember 2020[54] (ISG) 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 lässt nach Artikel 41 Absatz 2 ISG[55] die betroffene Person die Tätigkeit ausüben.

Art. 80 Abs. 2 Bst. c

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

c. nach Artikel 41 Absatz 2 ISG[56] die entscheidende Stelle die betroffene Person die Tätigkeit ausüben lässt.

7. Kernenergieverordnung vom 10. Dezember 2004[57]

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 …[58] über die Personensicherheitsprüfung (VPSP) geregelt.

2 Die Kosten für die Prüfung trägt die einleitende Stelle nach Artikel 15 Absatz 4 Buchstabe a VPSP.

53 SR **…**
54 SR **128**
55 SR **128**
56 SR **128**
57 SR **732.11**
58 SR **…**