Bundesgesetz
über die Informationssicherheit beim Bund
(Informationssicherheitsgesetz, ISG)

...

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,

gestützt auf die Artikel 54 Absatz 1, 60 Absatz 1, 101, 102 Absatz 1 und 173 Absatz 1 Buchstaben a und b sowie Absatz 2 der Bundesverfassung[1],

nach Einsicht in die Botschaft des Bundesrates vom ...[2],

beschliesst:

1. Kapitel: Allgemeine Bestimmungen

Art. 1 Zweck

[1] Dieses Gesetz soll die sichere Bearbeitung der Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz der Informatikmittel des Bundes gewährleisten.

[2] Dadurch sollen die folgenden öffentlichen Interessen geschützt werden:

a. die Entscheidungs- und Handlungsfähigkeit der Behörden und Organisationen des Bundes;

b. die innere und äussere Sicherheit der Schweiz;

c. die aussenpolitischen Interessen der Schweiz;

d. die wirtschafts-, finanz- und währungspolitischen Interessen der Schweiz;

e. die Erfüllung der gesetzlichen und vertraglichen Verpflichtungen der Behörden und Organisationen des Bundes zum Schutz von Informationen.

Art. 2 Verpflichtete Behörden und Organisationen

[1] Dieses Gesetz gilt für die nachstehenden Behörden (verpflichtete Behörden):

a. die Bundesversammlung;

b. den Bundesrat;

AS **...**

1 SR **101**

2 BBl **...**

c. die eidgenössischen Gerichte;

d. die Bundesanwaltschaft und die Aufsichtsbehörde der Bundesanwaltschaft;

e. die Schweizerische Nationalbank.

[2] Es gilt für die nachstehenden Organisationen (verpflichtete Organisationen):

a. die Parlamentsdienste;

b. die Bundesverwaltung;

c. die Verwaltungen der eidgenössischen Gerichte;

d. die Armee;

e. Organisationen nach Artikel 2 Absatz 4 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[3] (RVOG) für ihre Verwaltungsaufgaben.

[3] Der Bundesrat kann für Organisationen nach Artikel 2 Absätze 3 und 4 RVOG die Geltung des Gesetzes auf diejenigen Organisationen einschränken, die:

a. sicherheitsempfindliche Tätigkeiten ausüben; oder

b. zur Erfüllung ihrer Aufgaben Informatikmittel des Bundes einsetzen oder darauf zugreifen.

[4] Er kann die Geltung nach Absatz 3 auf Teile des Gesetzes beschränken. Er berücksichtigt dabei die Vollzugsautonomie der betreffenden Organisationen nach Massgabe ihrer Organisationserlasse.

[5] Für Organisationen des öffentlichen und privaten Rechts, die kritische Infrastrukturen betreiben, die aber nicht unter die Absätze 1−3 fallen, gelten die Artikel 75–81 dieses Gesetzes. Die Spezialgesetzgebung kann weitere Teile dieses Gesetzes für anwendbar erklären.

Art. 3 Geltung für die Kantone

[1] Für die Kantone gelten die Bestimmungen über klassifizierte Informationen und die Sicherheit beim Einsatz von Informatikmitteln, soweit sie im Rahmen der Zusammenarbeit mit dem Bund oder beim Vollzug von Bundesrecht klassifizierte Informationen des Bundes bearbeiten oder auf Informatikmittel des Bundes zugreifen.

[2] Die Bestimmungen gelten nicht, wenn die Kantone eine mindestens gleichwertige Informationssicherheit gewährleisten.

Art. 4 Verhältnis zu anderen Erlassen des Bundes

[1] Das Öffentlichkeitsgesetz vom 17. Dezember 2004[4] geht diesem Gesetz vor.

3 SR **172.010**

[2] Für Informationen, deren Schutz gleichzeitig in anderen Bundesgesetzen geregelt ist, finden die Bestimmungen dieses Gesetzes ergänzend Anwendung.

Art. 5 Begriffe

In diesem Gesetz bedeuten:

a. *Informatikmittel*: Mittel der Informations- und Kommunikationstechnik, namentlich Anwendungen, Informationssysteme und Datensammlungen sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen;

b. *sicherheitsempfindliche Tätigkeit*:

   1. die Bearbeitung von «vertraulich» oder «geheim» klassifizierten Informationen,

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

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

c. *kritische Infrastrukturen*: Informations-, Kommunikations-, Energie-, Transport- und weitere Infrastrukturen, die für das Funktionieren von Gesellschaft, Wirtschaft und Staat unerlässlich sind.

2. Kapitel: Allgemeine Massnahmen

1. Abschnitt: Grundsätze

Art. 6 Informationssicherheit

[1] Die verpflichteten Behörden und Organisationen sorgen dafür, dass der Schutzbedarf der Informationen, für die sie zuständig sind, hinsichtlich einer allfälligen Beeinträchtigung der Interessen nach Artikel 1 Absatz 2 beurteilt wird.

[2] Sie sorgen dafür, dass diese Informationen, ihrem Schutzbedarf entsprechend:

a. nur Berechtigten zugänglich sind (Vertraulichkeit);

b. verfügbar sind, wenn sie benötigt werden (Verfügbarkeit);

c. nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität);

d. nachvollziehbar bearbeitet werden (Nachvollziehbarkeit).

4 SR **152.3**

[3] Sie sorgen dafür, dass die Informatikmittel, die sie zur Erfüllung ihrer gesetzlichen Aufgaben einsetzen, vor Missbrauch und Störung geschützt werden.

[4] Sie tragen dabei den Grundsätzen der Zweckmässigkeit, der Wirtschaftlichkeit und der Benutzerfreundlichkeit Rechnung.

Art. 7 Oberste Führungsverantwortung

[1] Die verpflichteten Behörden sorgen in ihrem Zuständigkeitsbereich dafür, dass die Informationssicherheit nach dem Stand von Wissenschaft und Technik organisiert, umgesetzt und überprüft wird.

[2] Sie legen fest:

a. ihre Ziele für die Informationssicherheit;

b. die Eckwerte für den Umgang mit Risiken;

c. die Folgen bei Missachtung der Vorschriften.

Art. 8 Risikomanagement

[1] Die verpflichteten Behörden und Organisationen sorgen in ihrem Zuständigkeitsbereich dafür, dass die Risiken für die Informationssicherheit laufend beurteilt werden.

[2] Sie treffen die erforderlichen Massnahmen, um die Risiken zu vermeiden oder auf ein tragbares Mass zu reduzieren.

[3] Risiken, die getragen werden sollen, müssen nachweislich akzeptiert werden.

Art. 9 Zusammenarbeit mit Dritten

[1] Arbeiten die verpflichteten Behörden und Organisationen mit Dritten zusammen, so sorgen sie dafür, dass die Anforderungen und Massnahmen nach diesem Gesetz in den entsprechenden Vereinbarungen und Verträgen festgehalten werden.

[2] Sie sorgen für eine angemessene Überprüfung der Umsetzung der Massnahmen.

Art. 10 Vorgehen bei Verletzungen der Informationssicherheit

[1] Die verpflichteten Behörden und Organisationen sorgen dafür, dass Verletzungen der Informationssicherheit rasch erkannt, deren Ursachen abgeklärt und allfällige Auswirkungen minimiert werden.

[2] Die verpflichteten Behörden sorgen dafür, dass für allfällige schwerwiegende Verletzungen der Informationssicherheit, welche die Erfüllung unverzichtbarer Aufgaben des Bundes gefährden können, Vorsorgeplanungen erstellt und entsprechende Übungen durchgeführt werden.

2. Abschnitt: Klassifizierung von Informationen

Art. 11 Grundsätze der Klassifizierung

[1] Die verpflichteten Behörden und Organisationen sorgen dafür, dass Informationen, welche die Kriterien nach Artikel 13 erfüllen, klassifiziert werden.

[2] Die Klassifizierung ist auf das erforderliche Mindestmass zu beschränken und nach Möglichkeit zeitlich zu begrenzen.

Art. 12 Zuständigkeiten

[1] Die verpflichteten Behörden legen fest, welche Personen und Stellen für das Klassifizieren der Informationen zuständig sind (klassifizierende Stellen).

[2] Klassifizierungen dürfen nur von der klassifizierenden Stelle oder von der Stelle, die dieser übergeordnet ist, geändert oder aufgehoben werden.

[3] Der Bundesrat regelt die Entklassifizierung von Archivgut.

Art. 13 Klassifizierungsstufen

[1] Als «intern» werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte die Interessen nach Artikel 1 Absatz 2 Buchstaben a–d beeinträchtigen kann.

[2] Als «vertraulich» werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte die Interessen nach Artikel 1 Absatz 2 Buchstaben a–d erheblich beeinträchtigen kann.

[3] Als «geheim» werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte die Interessen nach Artikel 1 Absatz 2 Buchstaben a–d schwerwiegend beeinträchtigen kann.

[4] Die Klassifizierungsvermerke sind in Grossbuchstaben zu schreiben.

Art. 14 Zugang zu klassifizierten Informationen

[1] Zugang zu klassifizierten Informationen erhalten nur Personen, die Gewähr dafür bieten, dass sie damit sachgerecht umgehen, und:

a. die Informationen zur Erfüllung einer gesetzlichen Aufgabe benötigen; oder

b. über eine vertraglich vereinbarte Zugangsberechtigung verfügen und die Informationen zur Erfüllung der ihnen übertragenen Aufgaben benötigen.

[2] Der Zugang zu klassifiziertem Archivgut richtet sich nach den Bestimmungen der Archivierungsgesetzgebung.

[3] Vorbehalten bleiben durch völkerrechtliche Verträge nach Artikel 88 geregelte Zugangsbeschränkungen.

Art. 15 Zugang zu klassifizierten Informationen in besonderen Verfahren

[1] Der Zugang zu klassifizierten Informationen in der Bundesversammlung, in den Parlamentsdiensten sowie in den Gerichten und Staatsanwaltschaften richtet sich nach dem jeweils anwendbaren Verfahrensrecht.

[2] Vor dem Entscheid, den Zugang zu einer Information nach Absatz 1 zu ermöglichen, kann das zuständige parlamentarische Organ oder das zuständige Gericht die klassifizierende Stelle anhören.

3. Abschnitt: Sicherheit beim Einsatz von Informatikmitteln

Art. 16 Sicherheitsverfahren

[1] Die verpflichteten Behörden legen ein Verfahren zur Gewährleistung der Informationssicherheit beim Einsatz von Informatikmitteln fest (Sicherheitsverfahren).

[2] Das Sicherheitsverfahren umfasst insbesondere:

a. die Beurteilung des Schutzbedarfs der Informationen vor dem Einsatz von Informatikmitteln;

b. die Umsetzung von Sicherheitsmassnahmen und deren Überprüfung;

c. die Zuständigkeit für die Sicherheitsfreigabe von Informatikmitteln;

d. das Vorgehen bei Veränderung der Risiken.

[3] Für die Durchführung des Sicherheitsverfahrens ist die verpflichtete Behörde oder Organisation zuständig, die den Einsatz der Informatikmittel beschliesst.

Art. 17 Sicherheitsstufen

[1] Die Sicherheitsstufe «Grundschutz» gilt für sämtliche Informatikmittel, sofern diese nicht höher eingestuft werden müssen.

[2] Die Sicherheitsstufe «hoher Schutz» gilt für Informatikmittel, wenn:

a. eine Verletzung der Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit der Informationen, die damit bearbeitet werden, die Interessen nach Artikel 1 Absatz 2 erheblich beeinträchtigen kann;

b. ein Missbrauch oder eine Störung des Informatikmittels die Interessen nach Artikel 1 Absatz 2 erheblich beeinträchtigen kann.

[3] Die Sicherheitsstufe «sehr hoher Schutz» gilt für Informatikmittel, wenn:

a. eine Verletzung der Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit der Informationen, die damit bearbeitet werden, die Interessen nach Artikel 1 Absatz 2 schwerwiegend beeinträchtigen kann;

b. ein Missbrauch oder eine Störung des Informatikmittels die Interessen nach Artikel 1 Absatz 2 schwerwiegend beeinträchtigen kann.

Art. 18 Sicherheitsmassnahmen

[1] Die verpflichteten Behörden legen die Mindestanforderungen für die Sicherheitsstufen nach Artikel 17 fest.

[2] Die Mindestanforderungen der Sicherheitsstufe «Grundschutz» müssen sämtliche Informatikmittel erfüllen.

[3] Bei Informatikmitteln der Sicherheitsstufe «sehr hoher Schutz» muss die Wirksamkeit der Massnahmen periodisch geprüft werden.

Art. 19 Sicherheit beim Betrieb

[1] Die verpflichteten Behörden und Organisationen gewährleisten die Sicherheit der Informatikmittel, die sie für sich selbst oder im Auftrag einer anderen Behörde oder Organisation betreiben.

[2] Die Bearbeitung von Personendaten im Rahmen der Netzwerküberwachung richtet sich sinngemäss nach den Artikeln 57i–57q RVOG[5].

4. Abschnitt: Personelle Massnahmen

Art. 20 Voraussetzungen für den Zugang zu Informationen und Informatikmitteln des Bundes

[1] Die verpflichteten Behörden und Organisationen sorgen dafür, dass Personen, die Zugang zu Informationen, Informatikmitteln, Räumlichkeiten und anderen Infrastrukturen des Bundes haben:

a. sorgfältig ausgewählt werden;

b. risikogerecht identifiziert werden;

c. stufengerecht aus- und weitergebildet werden;

d. gegebenenfalls zur Geheimhaltung verpflichtet werden.

[2] Sie können biometrische Verifikationsmethoden verwenden, wenn dies zur risikogerechten Identifizierung von Personen erforderlich ist. Die biometrischen Daten werden nach dem Wegfall der Zugangsberechtigung vernichtet.

Art. 21 Restriktive Erteilung von Berechtigungen

[1] Die verpflichteten Behörden und Organisationen sorgen dafür, dass nur diejenigen Berechtigungen für den Zugang zu Informationen, Informatikmitteln, Räumlichkeiten und anderen Infrastrukturen des Bundes erteilt werden, welche die betreffenden Personen zur Erfüllung ihrer Aufgaben benötigen.

5 SR **172.010**

[2] Die Berechtigungen werden entzogen, sobald die Anstellung oder der Vertrag endet oder die Aufgabe erfüllt ist. Sie dürfen ohne Vorankündigung gesperrt oder entzogen werden, wenn konkrete Anhaltspunkte für eine Gefährdung der Sicherheit vorliegen.

5. Abschnitt: Physischer Schutz

Art. 22 Grundsatz

Die verpflichteten Behörden und Organisationen sorgen für einen angemessenen physischen Schutz der Informationen und Informatikmittel, für die sie zuständig sind, vor Missbrauch und Störung.

Art. 23 Sicherheitszonen

[1] Die verpflichteten Behörden und Organisationen können Räumlichkeiten und Bereiche als Sicherheitszone bezeichnen, in denen:

a. häufig «vertraulich» oder «geheim» klassifizierte Informationen bearbeitet werden; oder

b. Informatikmittel der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz» betrieben werden.

[2] Sie sind befugt:

a. das Mitführen bestimmter Gegenstände, insbesondere von Aufnahmegeräten, zu verbieten;

b. sicherheitsempfindliche Bereiche mit Aufnahmegeräten zu überwachen;

c. Taschen- und Personenkontrollen durchzuführen;

d. unangemeldet Raumkontrollen, auch in Abwesenheit der Angestellten, durchzuführen.

[3] Sie können in Sicherheitszonen, in denen «geheim» klassifizierte Informationen häufig bearbeitet oder Informatikmittel der Sicherheitsstufe «sehr hoher Schutz» betrieben werden, störende Fernmeldeanlagen nach Artikel 34 Absatz 1ter des Fernmeldegesetzes vom 30. April 1997[6] (FMG) betreiben.

[4] Vorbehalten bleiben die besonderen Vorschriften für Sicherheitszonen gemäss völkerrechtlichen Verträgen nach Artikel 88 sowie für Schutzzonen von Anlagen nach der Gesetzgebung über den Schutz militärischer Anlagen.

6 SR **784.10**

6. Abschnitt: Identitätsverwaltungs-Systeme

Art. 24 Einsatz von Identitätsverwaltungs-Systemen

1 Die verpflichteten Behörden können zur zentralen Verwaltung der Daten zur Identifizierung von Personen, die Zugang zu Informationen, Informatikmitteln, Räumlichkeiten und anderen Infrastrukturen haben, Informationssysteme betreiben (Identitätsverwaltungs-Systeme).

2 Die Identitätsverwaltungs-Systeme prüfen die Identität und berechtigungsbezogene Eigenschaften von Personen, Maschinen und Systemen. Sie übermitteln das Resultat an die angeschlossenen Informationssysteme, damit diese die Berechtigungen ermitteln können.

3 Die verpflichteten Behörden bezeichnen für jedes Identitätsverwaltungs-System eine verantwortliche Stelle.

Art. 25 Datenaustausch und -abgleich

1 Die Identitätsverwaltungs-Systeme können mit den angeschlossenen Informationssystemen, mit Personal- und Benutzerverzeichnissen und mit anderen Identitätsverwaltungs-Systemen von verpflichteten Behörden Daten austauschen und abgleichen.

2 Der Austausch und Abgleich ist auf die Daten zu begrenzen, die im jeweiligen System bearbeitet werden dürfen.

Art. 26 Verwendung der AHV-Versichertennummer

1 Die verantwortliche Stelle kann für die korrekte Zuordnung beim Abgleich von Personendaten die Versichertennummer nach Artikel 50*c* des Bundesgesetzes vom 20. Dezember 1946[7] über die Alters- und Hinterlassenenversicherung (AHV-Versichertennummer) im Identitätsverwaltungs-System vorübergehend verwenden, um eine nicht zurückrechenbare Personennummer zu erzeugen.

2 Die AHV-Versichertennummer wird unmittelbar nach der Berechnung der abgeleiteten Personennummer gelöscht.

Art. 27 Ausführungsbestimmungen

Die verpflichteten Behörden erlassen Ausführungsbestimmungen insbesondere über:

a. den Datenschutz und die Datensicherheit;

b. die bearbeiteten Personendaten;

c. den Datenaustausch und -abgleich mit anderen Systemen;

7 SR **831.10**

d. die Protokollierung und die Weitergabe von Protokolldaten an die angeschlossenen Informationssysteme;

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

3. Kapitel: Personensicherheitsprüfung

1. Abschnitt: Allgemeine Bestimmungen

Art. 28 Prüfzweck und Prüfungsinhalt

[1] Die Personensicherheitsprüfung dient zur Beurteilung, ob ein Risiko für die Informationssicherheit bestehen könnte, wenn eine Person im Rahmen ihrer Funktion oder eines Auftrags eine sicherheitsempfindliche Tätigkeit ausübt.

[2] Zu diesem Zweck werden sicherheitsrelevante Daten über die Lebensführung der zu prüfenden Person, insbesondere über ihre engen persönlichen Beziehungen und familiären Verhältnisse, ihre finanzielle Lage und ihre Beziehungen zum Ausland, bearbeitet.

[3] Daten über die Ausübung verfassungsmässiger Rechte dürfen nur dann bearbeitet werden, wenn ein konkreter Verdacht besteht, dass die zu prüfende Person diese Rechte ausübt, um Tätigkeiten vorzubereiten oder auszuüben, welche die Interessen nach Artikel 1 Absatz 2 erheblich beeinträchtigen können.

Art. 29 Funktionenliste

[1] Die verpflichteten Behörden erlassen für ihren Zuständigkeitsbereich eine Liste der Funktionen, welche die Ausübung einer sicherheitsempfindlichen Tätigkeit erfordern.

[2] Sie prüfen periodisch die Richtigkeit der Liste und passen sie an.

Art. 30 Zu prüfende Personen

[1] Eine Personensicherheitsprüfung wird bei Personen durchgeführt, die:

a. eine Funktion ausüben, die in einer Liste nach Artikel 29 enthalten ist;

b. als Angestellte eines Kantons im Rahmen der Zusammenarbeit mit dem Bund oder beim Vollzug von Bundesrecht eine sicherheitsempfindliche Tätigkeit ausüben;

c. für eine verpflichtete Behörde oder Organisation einen Auftrag ausführen, der die Ausübung einer sicherheitsempfindlichen Tätigkeit einschliesst;

d. aufgrund eines völkerrechtlichen Vertrags nach Artikel 88 einer Personensicherheitsprüfung unterzogen werden müssen.

[2] Soll eine Person von einer ausländischen Behörde oder internationalen Organisation mit der Ausübung einer sicherheitsempfindlichen Tätigkeit betraut werden, so

wird die Personensicherheitsprüfung durchgeführt, sofern die Schweiz mit dem betreffenden Staat oder der betreffenden internationalen Organisation einen völkerrechtlichen Vertrag nach Artikel 88 abgeschlossen hat.

[3] Personen, die eine Funktion ausüben, die noch nicht in einer Liste nach Artikel 29 enthalten ist, können mit Zustimmung der verpflichteten Behörde ausnahmsweise einer Personensicherheitsprüfung unterzogen werden. Die betreffende Liste muss bei nächster Gelegenheit angepasst werden.

[4] Nicht durchgeführt wird die Personensicherheitsprüfung bei Anwärterinnen und Anwärtern auf folgende Funktionen:

a. Mitglied der Bundesversammlung;

b. Mitglied des Bundesrates, Bundeskanzlerin oder Bundeskanzler;

c. Richterin oder Richter eines eidgenössischen Gerichts;

d. Bundesanwältin oder Bundesanwalt;

e. Mitglied der Aufsichtsbehörde über die Bundesanwaltschaft;

f. General;

g. Mitglied einer kantonalen Regierung sowie Richterin oder Richter eines kantonalen Gerichts.

Art. 31 Prüfstufen

Die verpflichteten Behörden ordnen den sicherheitsempfindlichen Tätigkeiten eine der folgenden Prüfstufen zu:

a. Grundsicherheitsprüfung: für sicherheitsempfindliche Tätigkeiten, bei deren vorschriftswidriger oder unsachgemässer Ausübung die Interessen nach Artikel 1 Absatz 2 erheblich beeinträchtigt werden können.

b. erweiterte Personensicherheitsprüfung: für sicherheitsempfindliche Tätigkeiten, bei deren vorschriftswidriger oder unsachgemässer Ausübung die Interessen nach Artikel 1 Absatz 2 schwerwiegend beeinträchtigt werden können.

2. Abschnitt: Durchführung

Art. 32 Zuständige Stellen

[1] Die verpflichteten Behörden und die Kantone legen fest, welche Stellen zuständig sind für:

a. die Einleitung der Personensicherheitsprüfungen (einleitende Stellen);

b. den Entscheid über die Ausübung der sicherheitsempfindlichen Tätigkeit (entscheidende Stellen).

[2] Der Bundesrat setzt für die Durchführung der Personensicherheitsprüfungen eine oder mehrere Fachstellen ein (Fachstellen PSP). Diese sind in ihrer Beurteilung weisungsungebunden.

Art. 33 Einwilligung und Mitwirkung

[1] Personensicherheitsprüfungen dürfen nur mit der Einwilligung der zu prüfenden Person durchgeführt werden.

[2] Stellungspflichtige sowie Angehörige der Armee und des Zivilschutzes dürfen ohne deren Einwilligung geprüft werden.

[3] Die zu prüfende Person ist verpflichtet, an der Feststellung des Sachverhalts mitzuwirken.

Art. 34 Zeitpunkt der Personensicherheitsprüfung

[1] Bei Personen nach Artikel 30 Absatz 1 Buchstaben a und b muss die Personensicherheitsprüfung eingeleitet werden, bevor die Funktion übertragen wird.

[2] Bei Personen nach Artikel 30 Absatz 1 Buchstabe a, die dem Bundesrat zur Wahl vorgeschlagen werden sollen, muss die Personensicherheitsprüfung abgeschlossen sein, bevor die Person zur Wahl vorgeschlagen wird.

[3] Bei Personen nach Artikel 30 Absatz 1 Buchstabe c muss die Personensicherheitsprüfung abgeschlossen sein, bevor sie mit der Ausübung der sicherheitsempfindlichen Tätigkeit beauftragt wird.

[4] Bei Personen nach Artikel 30 Absatz 1 Buchstabe d richtet sich der Zeitpunkt der Personensicherheitsprüfung nach den Bestimmungen des entsprechenden Vertrags.

Art. 35 Datenerhebung

[1] Die zuständige Fachstelle PSP kann für die Grundsicherheitsprüfung aus folgenden Quellen Daten über die zu prüfende Person erheben:

a. aus dem Strafregister;

b. bei den Strafbehörden durch Einholen von Auskünften und Akten über laufende, abgeschlossene oder eingestellte Strafverfahren;

c. bei den Sicherheitsorganen des Bundes, dem Nachrichtendienst des Bundes (NDB), den Organen der Armee sowie weiteren Organen des Bundes, sofern diese Daten bearbeiten, die für die Beurteilung des Sicherheitsrisikos erforderlich sind;

d. aus den Registern und Akten der Sicherheitsorgane der Kantone sowie der Polizei;

e. aus den Registern der Betreibungs- und Konkursbehörden;

f. aus den Akten bisheriger Personensicherheitsprüfungen;

g. aus öffentlich zugänglichen Quellen.

[2] Sie kann für die erweiterte Personensicherheitsprüfung zudem aus folgenden Quellen Daten erheben:

a. bei den eidgenössischen und kantonalen Steuerbehörden;

b. aus den Registern der Einwohnerkontrollen;

c. bei Finanzinstituten und Banken, mit welchen die zu prüfende Person Geschäftsbeziehungen unterhält;

d. durch Befragung der zu prüfenden Person.

[3] Ergeben sich gestützt auf die erhobenen Daten konkrete Hinweise auf ein Sicherheitsrisiko oder sind für die Beurteilung nicht genügend Daten über einen hinreichenden Zeitraum vorhanden, so kann die Fachstelle PSP die zu prüfende Person befragen. Sie kann mit der Einwilligung der zu prüfenden Person auch Dritte befragen; sie macht die Drittperson darauf aufmerksam, dass sie freiwillig Auskunft gibt.

[4] Daten über Dritte, die untrennbar mit Daten über die zu prüfende Person verbunden sind, dürfen nur bearbeitet werden, wenn dies für die Beurteilung des Sicherheitsrisikos unerlässlich ist. Die Fachstelle PSP informiert die betroffenen Dritten über die Bearbeitung.

Art. 36 Amtshilfe

[1] Müssen die Daten bei einer ausländischen Behörde oder internationalen Organisation erhoben werden, so erfolgt dies über die zuständige Behörde oder Organisation nach Artikel 35.

[2] Ergibt die Datenerhebung konkrete Hinweise auf das organisierte oder internationale Verbrechen, so konsultiert die Fachstelle PSP die kriminalpolizeilichen Zentralstellen des Bundes. Die Zentralstellen geben der Fachstelle PSP nur sicherheitsrelevante Personendaten bekannt.

Art. 37 Kostentragung

[1] Behörden und Organisationen des öffentlichen Rechts, bei denen Daten erhoben werden dürfen oder die am Verfahren mitwirken müssen, sind verpflichtet, unentgeltlich mitzuwirken.

[2] Entsteht für Dritte durch die Mitwirkung ein erheblicher Aufwand, so werden sie dafür entschädigt.

[3] Der Bund trägt die Kosten der Personensicherheitsprüfungen von Angestellten der Kantone nach Artikel 30 Absatz 1 Buchstabe b.

Art. 38 Einstellung

[1] Die Fachstelle PSP stellt das Prüfverfahren ein, wenn die zu prüfende Person ihre Einwilligung zurückzieht oder für die Funktion oder für den Auftrag nicht mehr in Frage kommt.

[2] Sie teilt die Einstellung des Prüfverfahrens der betreffenden Person und der einleitenden Stelle mit. Die betreffende Person gilt damit als nicht geprüft.

3. Abschnitt: Beurteilung des Sicherheitsrisikos

Art. 39 Sicherheitsrisiko

[1] Ein Sicherheitsrisiko besteht, wenn aufgrund der erhobenen Daten konkrete Anhaltspunkte vorliegen, dass die geprüfte Person die sicherheitsempfindliche Tätigkeit mit hoher Wahrscheinlichkeit vorschriftswidrig oder unsachgemäss ausüben wird.

[2] Die Wahrscheinlichkeit einer vorschriftswidrigen oder unsachgemässen Ausübung der sicherheitsempfindlichen Tätigkeit kann insbesondere dann als hoch gelten, wenn konkrete Anhaltspunkte für folgende persönliche Eigenschaften vorliegen:

a. mangelnde persönliche Integrität oder Vertrauenswürdigkeit;

b. Erpressbarkeit oder Bestechlichkeit; oder

c. beeinträchtigtes Urteils- oder Entscheidungsvermögen.

[3] Das Sicherheitsrisiko muss ungeachtet des Verschuldens der geprüften Person aufgrund der tatsächlichen Umstände ihrer persönlichen Verhältnisse festgestellt werden.

Art. 40 Ergebnis der Beurteilung

[1] Die Fachstelle PSP stellt das Ergebnis der Beurteilung als eine der folgenden Erklärungen mit der nachstehenden Bedeutung aus:

a. Sicherheitserklärung: Es besteht kein Sicherheitsrisiko.

b. Sicherheitserklärung mit Vorbehalt: Es besteht ein Sicherheitsrisiko, das mit Auflagen auf ein tragbares Mass reduziert werden kann. Die Fachstelle PSP empfiehlt entsprechende Auflagen.

c. Risikoerklärung: Es besteht ein Sicherheitsrisiko.

d. Feststellungserklärung: Für die Beurteilung des Sicherheitsrisikos sind nicht genügend Daten über einen hinreichenden Zeitraum vorhanden.

[2] Bevor die Fachstelle PSP eine Erklärung nach Absatz 1 Buchstaben b–d ausstellt, gibt sie der geprüften Person die Möglichkeit zur Stellungnahme.

Art. 41 Mitteilung

[1] Die Fachstelle PSP teilt ihre Erklärung der geprüften Person sowie der entscheidenden Stelle schriftlich mit.

[2] Bei den vom Bundesrat zu wählenden Personen teilt die Fachstelle PSP ihre Erklärung dem antragstellenden Departement mit.

[3] Sie kann einer anderen entscheidenden Stelle die Erklärung mitteilen, wenn die geprüfte Person:

a. für eine andere sicherheitsempfindliche Tätigkeit nach diesem Gesetz einer Personensicherheitsprüfung untersteht;

b. einer Prüfung der Vertrauenswürdigkeit nach einem anderen Bundesgesetz untersteht;

c. als Angehörige der Armee einer Prüfung nach Artikel 113 des Militärgesetzes vom 3. Februar 1995[8] (MG) untersteht.

[4] Liegen der Fachstelle PSP bereits vor Abschluss der Beurteilung konkrete Anhaltspunkte vor, dass ein Sicherheitsrisiko bestehen könnte, so kann sie den Stellen nach den Absätzen 1–3 sowie der zu prüfenden Person die vorläufigen Erkenntnisse schriftlich mitteilen.

4. Abschnitt: Folgen der Erklärung

Art. 42 Ausübung der sicherheitsempfindlichen Tätigkeit

[1] Die Erklärungen der Fachstellen PSP haben empfehlenden Charakter.

[2] Die entscheidende Stelle entscheidet gestützt auf die Erklärung, ob die geprüfte Person die sicherheitsempfindliche Tätigkeit ausüben darf.

[3] Sie kann die Ausübung der sicherheitsempfindlichen Tätigkeit mit Auflagen verbinden.

[4] Sie teilt ihren Entscheid der Fachstelle PSP mit.

Art. 43 Mehrmalige Verwendung einer Erklärung

Auf die Durchführung der Personensicherheitsprüfung kann verzichtet werden, wenn für die betreffende Person bereits eine Erklärung derselben oder der höheren Prüfstufe ausgestellt wurde:

a. für eine andere sicherheitsempfindliche Tätigkeit nach diesem Gesetz;

b. im Rahmen einer Prüfung der Vertrauenswürdigkeit nach einem anderem Bundesgesetz.

Art. 44 Wiederholung

[1] Die Personensicherheitsprüfung wird wie folgt wiederholt:

a. Grundsicherheitsprüfung: frühestens nach fünf, spätestens aber nach zehn Jahren;

b. erweiterte Personensicherheitsprüfung: frühestens nach drei, spätestens aber nach fünf Jahren.

[2] Der Bundesrat kann für Funktionen der Armee und des Zivilschutzes von der Wiederholung der Grundsicherheitsprüfung absehen.

8 SR **510.10**

[3] Hat die einleitende oder die entscheidende Stelle Grund anzunehmen, dass seit der letzten Prüfung neue Risiken entstanden sind, so kann sie bei der zuständigen Fachstelle PSP mit schriftlicher Begründung eine Wiederholung der Personensicherheitsprüfung verlangen.

Art. 45 Rechtsschutz

[1] Die geprüfte Person hat nach Erhalt der Erklärung nach Artikel 40 Absatz 1 30 Tage Zeit, um:

a. Einsicht in die Prüfungsunterlagen zu nehmen;

b. die Berichtigung falscher Daten oder die Vernichtung nicht mehr aktueller Daten zu verlangen;

c. einen Bestreitungsvermerk anbringen zu lassen.

[2] Die Einschränkung des Auskunftsrechts richtet sich nach Artikel 9 des Bundesgesetzes vom 19. Juni 1992[9] über den Datenschutz (DSG).

[3] Die Erklärung stellt einen Realakt nach Artikel 25*a* des Verwaltungsverfahrensgesetzes vom 20. Dezember 1968[10] dar. Die geprüfte Person kann gegen eine Erklärung nach Artikel 40 Absatz 1 Buchstaben b−d innerhalb von 30 Tagen nach deren Mitteilung beim Bundesverwaltungsgericht Beschwerde führen.

[4] Ist das Bundesgericht oder das Bundesverwaltungsgericht die entscheidende Stelle, so gilt Artikel 36 Absätze 2 und 4 des Bundespersonalgesetzes vom 24. März 2000[11] sinngemäss.

[5] Das Beschwerdeverfahren richtet sich im Übrigen nach den allgemeinen Bestimmungen über die Bundesrechtspflege.

5. Abschnitt: Bearbeitung von Personendaten

Art. 46 Informationssystem zur Personensicherheitsprüfung

[1] Die Fachstellen PSP betreiben zur Durchführung der Personensicherheitsprüfungen ein Informationssystem.

[2] Jede Fachstelle PSP ist für die rechtmässige Bearbeitung der Personendaten im Informationssystem verantwortlich.

[3] Im Informationssystem können besonders schützenswerte Personendaten und Persönlichkeitsprofile nach Artikel 3 Buchstaben c und d DSG[12] bearbeitet werden, sofern dies zur Beurteilung des Sicherheitsrisikos erforderlich ist.

9 SR **235.1**
10 SR **172.021**
11 SR **172.220.1**

[4] Das Informationssystem enthält folgende Daten und Angaben:

a. Daten zur Identität der zu prüfenden oder geprüften Personen, einschliesslich der AHV-Versichertennummer und der Passnummer;

b. die Daten nach den Artikeln 35 und 36;

c. die Beurteilung des Sicherheitsrisikos;

d. die Erklärung nach Artikel 40 Absatz 1;

e. den Entscheid der entscheidenden Stelle;

f. Daten und Akten aus Beschwerdeverfahren;

g. Listen und Statistiken, die Daten nach den Buchstaben a–f enthalten.

[5] Werden Daten nach Absatz 4 ausserhalb des Informationssystems bearbeitet, so muss dies im Informationssystem vermerkt werden.

[6] Die Daten nach Absatz 4 können automatisch und systematisch durch Abfrage der folgenden Informationssysteme erhoben werden:

a. Strafregister-Informationssystem VOSTRA nach den Artikeln 365–371*a* des Strafgesetzbuchs[13];

b. nationaler Polizeiindex nach Artikel 17 des Bundesgesetzes vom 13. Juni 2008[14] über die polizeilichen Informationssysteme des Bundes;

c. INDEX NDB nach Artikel 51 des Nachrichtendienstgesetzes vom 25. September 2015[15];

Art. 47 Zugriffsrechte und Datenbekanntgabe

[1] Die folgenden Stellen haben im Abrufverfahren Zugriff auf die nachstehenden Daten im Informationssystem:

a. einleitende Stellen: auf die Daten nach Artikel 46 Absatz 4 Buchstabe b, die sie anlässlich der Einleitung der Prüfung selber erfasst haben, sowie die Daten nach Artikel 46 Absatz 4 Buchstaben a, d und e;

b. entscheidende Stellen: auf die Daten nach Artikel 46 Absatz 4 Buchstaben a, d und e;

c. Informationssicherheitsbeauftragte nach Artikel 82 zur Erfüllung ihrer Kontrollaufgaben: auf die Daten nach Artikel 46 Absatz 4 Buchstaben a, d und e;

d. Stellen des Bundes und der Kantone, bei denen Daten nach Artikel 38 erhoben werden: auf die Daten nach Artikel 46 Absatz 4 Buchstabe a.

12 SR **235.1**
13 SR **311.0**
14 SR **361**
15 SR **121**

[2] Die folgenden Stellen haben über eine Schnittstelle Zugriff auf die nachstehenden Daten im Informationssystem:

a. die Fachstelle nach Artikel 52 Absatz 2 zur Durchführung des Betriebssicherheitsverfahrens nach den Artikeln 50–74 über das Informationssystem nach Artikel 71: auf die Daten nach Artikel 46 Absatz 4 Buchstaben a, d und e;

b. die Gruppe Verteidigung:

1. zur Erfüllung ihrer Aufgaben nach Artikel 13 des Bundesgesetzes vom 3. Oktober 2008[16] über die militärischen Informationssysteme (MIG) über das Personalinformationssystem der Armee nach Artikel 12 MIG: auf die Daten nach Artikel 46 Absatz 4 Buchstaben a, d und e,

2. zur Erfüllung ihrer Aufgaben nach Artikel 19 MIG über das Informationssystem Rekrutierung nach Artikel 18 MIG: auf die Daten nach Artikel 46 Absatz 4 Buchstaben a und e,

3. zur Erfüllung ihrer Aufgaben nach Artikel 157 MIG über das Informationssystem Besuchsanträge nach Artikel 156 MIG: auf die Daten nach Artikel 46 Absatz 4 Buchstaben a und e,

4. zur Erfüllung ihrer Aufgaben nach Artikel 163 MIG über das Informationssystem Zutrittskontrolle nach Artikel 162 MIG: auf die Daten nach Artikel 46 Absatz 4 Buchstaben a und e;

c. die Stelle, die für die Sicherheitsbescheinigung im internationalen Verhältnis nach Artikel 49 Buchstabe c zuständig ist: auf die Daten nach Artikel 46 Absatz 4 Buchstaben a, d und e.

[3] Die Fachstellen PSP können zudem Daten nach Artikel 46 Absatz 4 Buchstaben a und e weiteren Stellen des Bundes bekanntgeben, sofern dies zur Kontrolle des Zutritts zu einer Sicherheitszone erforderlich ist.

[4] Sie können den verpflichteten Behörden und Organisationen Listen und Statistiken nach Artikel 46 Absatz 1 Buchstabe g bekanntgeben, sofern dies zur Erfüllung von deren Kontrollaufgaben nach diesem Gesetz erforderlich ist.

Art. 48 Datenaufbewahrung, -archivierung und -vernichtung

[1] Die Fachstellen PSP können Befragungen nach Artikel 35 Absätze 2 Buchstabe d und 3 mit technischen Geräten aufnehmen und auf Datenträgern aufbewahren.

[2] Sie bewahren die Daten so lange auf, wie die betreffende Person die sicherheitsempfindliche Tätigkeit ausübt, längstens jedoch zehn Jahre.

[3] Die Archivierung der Daten richtet sich nach den Vorschriften der Archivierungsgesetzgebung.

16 SR **510.91**

[4] Wird das Prüfverfahren eingestellt, tritt eine geprüfte Person die vorgesehene Funktion nicht an oder lehnt sie den Auftrag ab, so werden alle mit der Personensicherheitsprüfung zusammenhängenden Daten und Akten spätestens nach drei Monaten vernichtet.

6. Abschnitt: Bestimmungen des Bundesrats

Art. 49

Der Bundesrat regelt:

a. das Verfahren der Personensicherheitsprüfung;

b. die Organisation der Fachstellen PSP;

c. die Sicherheitsbescheinigung für Personen im internationalen Verhältnis;

d. die Verantwortung für den Datenschutz in Zusammenhang mit dem Informationssystem nach Artikel 46 sowie die Datensicherheit;

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

4. Kapitel: Betriebssicherheitsverfahren

1. Abschnitt: Allgemeine Bestimmungen

Art. 50 Verfahrenszweck

Das Betriebssicherheitsverfahren dient zur Gewährleistung der Informationssicherheit bei der Erfüllung von öffentlichen Aufträgen durch Unternehmen und Subunternehmen oder Teile davon (Betriebe), sofern die Aufträge die Ausübung einer sicherheitsempfindlichen Tätigkeit einschliessen (sicherheitsempfindliche Aufträge).

Art. 51 Betroffene Betriebe

[1] Das Betriebssicherheitsverfahren kann durchgeführt werden bei Betrieben:

a. die einen sicherheitsempfindlichen Auftrag einer verpflichteten Behörde oder Organisation ausführen sollen;

b. mit Sitz in der Schweiz, die sich um einen Auftrag bewerben, für den sie eine Betriebssicherheitsbescheinigung nach Artikel 67 benötigen.

[2] Das Verfahren darf nur mit Einwilligung des Betriebs durchgeführt werden.

[3] Die Betriebe nach Absatz 1 Buchstabe b tragen die Kosten des Verfahrens.

Art. 52 Einstellung des Verfahrens

[1] Das Betriebssicherheitsverfahren wird eingestellt, wenn der Betrieb:

a. seine Einwilligung zurückzieht oder am Verfahren nicht mitwirkt;

b. sein Angebot zurückzieht;

c. für den Auftrag nicht mehr in Frage kommt.

[2] Die für die Durchführung des Betriebssicherheitsverfahrens zuständige Fachstelle (Fachstelle BS) teilt dem Betrieb und der den Auftrag vergebenden Behörde oder Organisation (Auftraggeberin) die Einstellung des Verfahrens mit.

2. Abschnitt: Einleitung des Betriebssicherheitsverfahrens

Art. 53 Antrag auf Einleitung

[1] Verpflichtete Behörden und Organisationen beantragen der Fachstelle BS die Einleitung des Verfahrens, wenn sie beabsichtigen, einen sicherheitsempfindlichen Auftrag zu vergeben.

[2] Die verpflichteten Behörden legen fest, welche Stellen für die Antragstellung zuständig sind.

[3] Für Betriebe nach Artikel 51 Absatz 1 Buchstabe b stellt die zuständige ausländische Behörde oder internationale Organisation den Antrag.

Art. 54 Prüfung des Antrags

[1] Die Fachstelle BS prüft den Antrag und leitet das Verfahren ein.

[2] Sie kann im Einvernehmen mit der Auftraggeberin auf die Einleitung verzichten, wenn das Sicherheitsrisiko mit anderen Massnahmen auf ein tragbares Mass reduziert werden kann. Sie empfiehlt entsprechende Massnahmen.

Art. 55 Festlegung der Sicherheitsanforderungen

Die Fachstelle BS legt in Absprache mit der Auftraggeberin die Anforderungen an die Informationssicherheit für das Vergabeverfahren und die Auftragserfüllung fest.

3. Abschnitt: Beurteilung der Betriebe

Art. 56 Eignung

[1] Die Auftraggeberin teilt der Fachstelle BS mit, welche Betriebe für die Ausführung des sicherheitsempfindlichen Auftrags in Frage kommen.

[2] Die Fachstelle BS beurteilt, ob diese Betriebe zur Ausführung des sicherheitsempfindlichen Auftrags geeignet sind oder ob ein Sicherheitsrisiko besteht.

[3] Sie ist in ihrer Beurteilung weisungsungebunden.

Art. 57 Datenerhebung

[1] Die Fachstelle BS kann zur Beurteilung der Eignung Daten erheben:

a. beim Betrieb;

b. beim NDB;

c. aus öffentlich zugänglichen Quellen.

[2] Sie kann ausländische und internationale Dienststellen um die Zustellung entsprechender Daten ersuchen. Anfragen an ausländische Nachrichtendienste erfolgen über den NDB.

Art. 58 Sicherheitsrisiko

[1] Ein Sicherheitsrisiko besteht, wenn aufgrund der erhobenen Daten konkrete Anhaltspunkte vorliegen, dass der Betrieb den sicherheitsempfindlichen Auftrag mit hoher Wahrscheinlichkeit vorschriftswidrig oder unsachgemäss ausführen wird.

[2] Die Wahrscheinlichkeit einer vorschriftswidrigen oder unsachgemässen Ausführung des sicherheitsempfindlichen Auftrags kann insbesondere dann als hoch gelten, wenn:

a. der Betrieb mangelnde Integrität oder Vertrauenswürdigkeit aufweist;

b. der Betrieb von ausländischen Staaten oder Organisationen des öffentlichen oder privaten Rechts kontrolliert oder beeinflusst wird und diese Kontrolle oder dieser Einfluss nicht mit dem Schutz der Interessen nach Artikel 1 Absatz 2 vereinbar ist;

c. für Personen des Betriebs, die für die Ausführung des sicherheitsempfindlichen Auftrags unentbehrlich sind, eine Risikoerklärung ausgestellt wurde.

[3] Das Sicherheitsrisiko muss ungeachtet eines Verschuldens aufgrund der tatsächlichen Umstände und Verhältnisse des betroffenen Betriebs festgestellt werden.

Art. 59 Eröffnung der Beurteilung und Ausschluss aus dem Vergabeverfahren

[1] Die Fachstelle BS teilt ihre Beurteilung der Auftraggeberin mit und eröffnet sie dem Betrieb durch Verfügung.

[2] Kommt die Fachstelle BS zum Schluss, dass die Ausführung des sicherheitsempfindlichen Auftrags mit einem Sicherheitsrisiko verbunden ist, so schliesst die Auftraggeberin den Betrieb vom Vergabeverfahren aus.

[3] Ist die Ausführung des sicherheitsempfindlichen Auftrags bei allen in Frage kommenden Betrieben mit einem Sicherheitsrisiko verbunden, so kann die Auftraggeberin trotzdem einem dieser Betriebe den Auftrag erteilen. Die Fachstelle BS stellt das Betriebssicherheitsverfahren ein. Die Auftraggeberin wendet die Massnahmen nach den Artikeln 60, 61, 64 und 65 analog an.

4. Abschnitt: Sicherheitskonzept

Art. 60 Zuschlag und Sicherheitskonzept

[1] Die Auftraggeberin teilt der Fachstelle BS mit, welcher Betrieb den Zuschlag erhält.

[2] Der Betrieb erstellt nach den Vorgaben der Fachstelle BS ein Sicherheitskonzept.

[3] Die Fachstelle BS prüft das Sicherheitskonzept. Sie kann die dazu erforderlichen Daten schriftlich erheben oder den Betrieb inspizieren.

Art. 61 Personensicherheitsprüfungen

[1] Personen des Betriebs, die für eine sicherheitsempfindliche Tätigkeit vorgesehen sind, werden einer Personensicherheitsprüfung unterzogen.

[2] Die Fachstelle BS ist für den Entscheid nach Artikel 42 Absatz 2 zuständig. Wird das Verfahren eingestellt, weil sich kein Betrieb für die Ausführung des Auftrags eignet (Art. 59 Abs. 3), so ist die Auftraggeberin für den Entscheid zuständig.

5. Abschnitt: Betriebssicherheitserklärung

Art. 62 Ausstellung der Betriebssicherheitserklärung

[1] Die Fachstelle BS stellt dem Betrieb eine Betriebssicherheitserklärung in Form einer Verfügung aus, sobald dieser das Sicherheitskonzept nachweislich umgesetzt hat.

[2] Sie verweigert dem Betrieb die Betriebssicherheitserklärung und stellt das Betriebssicherheitsverfahren ein, wenn er das Sicherheitskonzept nicht umsetzt. Sie erlässt eine entsprechende Verfügung.

[3] Die Verfügungen nach den Absätzen 1 und 2 werden der Auftraggeberin mitgeteilt.

[4] Die Auftraggeberin ist an die Verfügung der Fachstelle BS gebunden; vorbehalten bleibt Artikel 59 Absatz 3.

[5] Die Gültigkeit der Betriebssicherheitserklärung beträgt fünf Jahre.

Art. 63 Ausführung des sicherheitsempfindlichen Auftrags

Die Auftraggeberin darf den sicherheitsempfindlichen Auftrag erst ausführen lassen, wenn die Fachstelle BS die Betriebssicherheitserklärung ausgestellt hat.

Art. 64 Pflichten des Betriebs

[1] Betriebe, die über eine Betriebssicherheiterklärung verfügen, müssen die Massnahmen des Sicherheitskonzepts laufend umsetzen.

[2] Sie melden der Fachstelle BS und der Auftraggeberin unverzüglich alle sicherheitsrelevanten Änderungen und Vorfälle.

Art. 65 Kontrollen und Schutzmassnahmen

[1] Die Fachstelle BS ist befugt:

a. Bereiche, in denen der sicherheitsempfindliche Auftrag ausgeführt wird, ohne Vorankündigung zu inspizieren;

b. auftragsrelevante Unterlagen einzusehen.

[2] Liegen konkrete Anhaltspunkte vor, dass die Informationssicherheit in einem Betrieb gefährdet ist, so kann die Fachstelle BS umgehend die erforderlichen Schutzmassnahmen treffen und insbesondere Unterlagen und Material sicherstellen.

Art. 66 Vereinfachtes Verfahren bei der Vergabe weiterer sicherheitsempfindlicher Aufträge

Betriebe, die über eine Betriebssicherheitserklärung verfügen, gelten für weitere sicherheitsempfindliche Aufträge als geeignet. Die Fachstelle BS prüft, ob das Sicherheitskonzept angepasst werden muss.

Art. 67 Internationale Betriebssicherheitsbescheinigung

Die Fachstelle BS stellt dem Betrieb auf dessen Antrag hin eine internationale Betriebssicherheitsbescheinigung aus.

Art. 68 Widerruf der Betriebssicherheitserklärung

[1] Die Fachstelle BS widerruft die Betriebssicherheitserklärung, wenn:

a. der Betrieb seine Pflichten nach Artikel 64 nicht erfüllt;

b. sich im Rahmen einer Wiederholung des Verfahrens ein Sicherheitsrisiko ergibt.

[2] Sie teilt ihre Verfügung dem Betrieb und der Auftraggeberin mit.

[3] Wird die Betriebssicherheitserklärung widerrufen, so zieht die Auftraggeberin den Auftrag umgehend zurück; vorbehalten bleibt Artikel 59 Absatz 3. Der Betrieb hat keinen Anspruch auf Entschädigung.

6. Abschnitt: Wiederholung des Verfahrens und Rechtsschutz

Art. 69 Wiederholung des Verfahrens

Das Betriebssicherheitsverfahren wird wiederholt, wenn:

a. im Zeitpunkt des Ablaufs der Gültigkeit der Betriebssicherheitserklärung ein sicherheitsempfindlicher Auftrag hängig ist;

b. konkrete Anhaltspunkte vorliegen, dass in Folge wesentlicher Änderungen im Betrieb neue Sicherheitsrisiken entstanden sind.

Art. 70 Rechtsschutz

[1] Der Betrieb hat nach Eröffnung einer Verfügung der Fachstelle BS 30 Tage Zeit, um:

a. Einsicht in die Unterlagen zu nehmen;

b. die Berichtigung falscher Daten oder die Vernichtung nicht mehr aktueller Daten zu verlangen;

c. einen Bestreitungsvermerk anbringen zu lassen;

d. beim Bundesverwaltungsgericht Beschwerde zu führen.

[2] Die Einschränkung des Auskunftsrechts richtet sich nach Artikel 9 DSG[17].

7. Abschnitt: Bearbeitung von Personendaten

Art. 71 Informationssystem zum Betriebssicherheitsverfahren

[1] Die Fachstelle BS betreibt zur Durchführung und Bewirtschaftung des Betriebssicherheitsverfahrens ein Informationssystem.

[2] Im Informationssystem können besonders schützenswerte Personendaten und Persönlichkeitsprofile nach Artikel 3 Buchstaben c und d DSG[18] bearbeitet werden, sofern dies zur Durchführung des Betriebssicherheitsverfahrens erforderlich ist.

[3] Das Informationssystem enthält folgende Daten und Angaben:

a. die Daten nach den Artikeln 57 und 60 Absatz 3;

b. das Ergebnis der Beurteilung nach Artikel 56 Absatz 2;

c. die Ergebnisse der für das Betriebssicherheitsverfahren erforderlichen Personensicherheitsprüfungen nach Artikel 61 Absatz 1;

d. den Entscheid der Fachstelle BS nach Artikel 61 Absatz 2;

e. die Namen aller Betriebe mit einer Betriebssicherheitserklärung;

f. die Massnahmen allfälliger Kontrollen nach Artikel 65;

g. Daten und Akten aus Beschwerdeverfahren.

[4] Die Fachstelle BS ist für die Sicherheit des Informationssystems sowie die rechtmässige Bearbeitung der Personendaten verantwortlich.

17 SR **235.1**
18 SR **235.1**

Art. 72 Zugriffsrechte und Datenbekanntgabe

[1] Die folgenden Stellen haben im Abrufverfahren Zugriff auf die nachstehenden Daten:

a. Auftraggeberinnen: auf die Daten nach Artikel 71 Absatz 3 Buchstaben b und d–g;

b. betroffene Betriebe, sofern sie vom Bundesrat gestützt auf Artikel 32 Absatz 1 Buchstabe a ermächtigt worden sind, in ihrem Zuständigkeitsbereich Personensicherheitsprüfungen einzuleiten: auf die Daten nach Artikel 71 Absatz 3 Buchstabe d.

[2] Die Fachstelle BS kann zudem Daten nach Artikel 71 Absatz 3 Buchstaben b–d weiteren Stellen des Bundes bekanntgeben, sofern dies zur Gewährleistung der Informationssicherheit erforderlich ist.

Art. 73 Datenaufbewahrung, -archivierung und -vernichtung

[1] Die Fachstelle BS bewahrt die Daten so lange auf, wie der betroffene Betrieb im Besitz einer Betriebssicherheitserklärung ist, längstens jedoch zehn Jahre.

[2] Die Archivierung der Daten richtet sich nach den Vorschriften der Archivierungsgesetzgebung.

[3] Wird das Betriebssicherheitsverfahren eingestellt, so werden alle damit zusammenhängenden Daten und Akten spätestens nach drei Monaten vernichtet.

8. Abschnitt: Bestimmungen des Bundesrats

Art. 74

Der Bundesrat regelt:

a. das Betriebssicherheitsverfahren im Einzelnen;

b. die Anwendung des Betriebssicherheitsverfahrens auf Subunternehmen;

c. die Organisation der Fachstelle BS;

d. die Datensicherheit im Informationssystem nach Artikel 71;

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

5. Kapitel: Kritische Infrastrukturen

Art. 75 Aufgaben des Bundes

[1] Der Bund unterstützt die Betreiberinnen von kritischen Infrastrukturen, um zu gewährleisten, dass Netz- und Systemunterbrechungen sowie Missbräuche selten, von kurzer Dauer und beherrschbar sind und das Schadensausmass gering ist.

[2] Die Unterstützung im Bereich der Informationssicherheit umfasst:

a. die frühzeitige Identifizierung und Bewertung von Bedrohungen, Gefahren, Schwachstellen und Sicherheitslücken;

b. die Erkennung von Vorfällen;

c. die Erhaltung und Wiederherstellung der Informationssicherheit nach einem Vorfall;

d. die Nachbearbeitung von Vorfällen.

[3] Der Bund führt einen nationalen Frühwarndienst und eine Anlaufstelle für präventive und reaktive Massnahmen im Bereich der technischen Informationssicherheit.

[4] Er sorgt dafür, dass die Betreiberinnen von kritischen Infrastrukturen mit den zuständigen Stellen des Bundes sowie gegenseitig Informationen sicher austauschen können.

[5] Der Bundesrat bezeichnet die für diese Aufgaben zuständigen Stellen des Bundes.

Art. 76 Bearbeitung von Personendaten

[1] Die Stellen nach Artikel 75 Absatz 5 können zur Erfüllung ihrer Aufgaben Adressierungselemente nach Artikel 3 Buchstabe f FMG[19] und damit zusammenhängende Personendaten bearbeiten.

[2] Sie können die Daten nach Absatz 1 auch bearbeiten, wenn diese:

a. Informationen über religiöse, weltanschauliche oder politische Ansichten enthalten; die Bearbeitung ist nur zulässig, wenn sie für die Bewertung von konkreten Bedrohungen und Gefahren im Bereich der Informationssicherheit erforderlich ist;

b. Informationen über administrative oder strafrechtliche Verfolgungen und Sanktionen enthalten.

[3] Die Personendaten können bearbeitet werden, ohne dass dies für die betroffenen Personen ersichtlich ist.

[4] Liegen konkrete Hinweise auf den Missbrauch einer Identität oder auf die unberechtigte Verwendung von Adressierungselementen vor, so sind die betroffenen Personen zu informieren. Vorbehalten bleiben die Artikel 18*a* Absatz 4 Buchstabe b und 18*b* DSG[20].

Art. 77 Zusammenarbeit im Inland

[1] Die Stellen nach Artikel 75 Absatz 5 können den Betreiberinnen von kritischen Infrastrukturen Personendaten nach Artikel 76 bekanntgeben, sofern dies zur Ge-

19 SR **784.10**
20 SR **235.1**

währleistung der Informationssicherheit zweckmässig ist.

[2] Sie können den Anbieterinnen und Betreiberinnen von Informatik- und Kommunikationsdiensten Personendaten nach Artikel 76 bekanntgeben, sofern dies zur Gewährleistung der Informationssicherheit von kritischen Infrastrukturen erforderlich ist.

[3] Die Betreiberinnen von kritischen Infrastrukturen sowie die Anbieterinnen und Betreiberinnen von Informatik- und Kommunikationsdiensten können den Stellen nach Artikel 75 Absatz 5 Daten, einschliesslich Personendaten, die sich auf einen bestimmten Vorfall beziehen, bekanntgeben. Die Stellen nach Artikel 75 Absatz 5 dürfen diese Daten nur mit ausdrücklicher Einwilligung der Datenlieferantinnen zu Strafverfolgungszwecken weitergeben.

Art. 78 Internationale Zusammenarbeit

[1] Die Stellen nach Artikel 75 Absatz 5 können mit ausländischen und internationalen Stellen, die für den Schutz kritischer Infrastrukturen zuständig sind, Daten nach Artikel 76 austauschen, wenn sie diese Daten für die Erfüllung von Aufgaben benötigen, die den Aufgaben nach Artikel 75 entsprechen.

[2] Der Datenaustausch nach Absatz 1 ist nur dann zulässig, wenn die ausländischen und internationalen Stellen die bestimmungsgemässe Verwendung gewährleisten.

[3] Werden die Daten für ein rechtliches Verfahren im Ausland benötigt, so gelten die Bestimmungen über die Amts- und Rechtshilfe.

Art. 79 Informationssystem zur Unterstützung von kritischen Infrastrukturen

[1] Die Stellen nach Artikel 75 Absatz 5 betreiben ein Informationssystem, um den sicheren Austausch von Informationen mit den Betreiberinnen von kritischen Infrastrukturen zu gewährleisten.

[2] Das Informationssystem enthält folgende Informationen:

a. Beschreibungen und Einschätzungen von Bedrohungen und Gefahren;
b. Anweisungen zur technischen Erkennung und Behebung von Vorfällen;
c. Vorfallanalysen und Sicherheitsempfehlungen;
d. Analysen betreffend Schwachstellen von Informatikmitteln;
e. Korrespondenz.

[3] Die Informationen nach Absatz 2 können auch Personendaten nach Artikel 76 enthalten.

Art. 80 Datenaufbewahrung und -archivierung

[1] Die Stellen nach Artikel 75 Absatz 5 bewahren Personendaten nur so lange auf, wie dies zur Abwehr von Gefahren oder zur Erkennung von Vorfällen zweckmässig ist, höchstens jedoch fünf Jahre.

[2] Die Archivierung der Daten richtet sich nach den Vorschriften der Archivierungsgesetzgebung.

Art. 81 Bestimmungen des Bundesrats

Der Bundesrat regelt:

a. die Aufgabenteilung, die Zusammenarbeit und den Austausch von Informationen zwischen den Stellen nach Artikel 75 Absatz 5 und dem NDB;

b. die Bekanntgabe von Informationen an Betreiberinnen von kritischen Infrastrukturen, Dritte sowie ausländische und internationale Stellen;

c. die Verantwortung für den Datenschutz in Zusammenhang mit dem Informationssystem nach Artikel 79 sowie die Datensicherheit;

d. die periodische Kontrolle der Bearbeitung von Personendaten im Informationssystem nach Artikel 79 durch eine externe Stelle.

6. Kapitel: Organisation und Vollzug

1. Abschnitt: Organisation

Art. 82 Informationssicherheitsbeauftragte

[1] Die folgenden Behörden und Organisationen bezeichnen für ihren Zuständigkeitsbereich eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten sowie eine Stellvertreterin oder einen Stellvertreter:

a. Bundesrat;

b. Verwaltungsdelegation der Bundesversammlung;

c. eidgenössische Gerichte;

d. Bundesanwaltschaft;

e. Schweizerische Nationalbank;

f. Departemente und Bundeskanzlei.

[2] Die Informationssicherheitsbeauftragten haben folgende Aufgaben:

a. Sie beraten und unterstützen die zuständigen Stellen in ihrem Bereich bei der Erfüllung ihrer Aufgaben und Pflichten nach diesem Gesetz.

b. Sie steuern im Auftrag ihrer Behörde oder Organisation die Fachorganisation der Informationssicherheit sowie das entsprechende Risikomanagement.

c. Sie überprüfen im Auftrag ihrer Behörde oder Organisation die Einhaltung der Vorgaben der Informationssicherheit, erstatten Bericht und beantragen die erforderlichen Massnahmen.

d. Sie können der Fachstelle des Bundes für Informationssicherheit sowie den Stellen nach Artikel 75 Absatz 5 sicherheitsrelevante Vorfälle melden.

[3] Den Informationssicherheitsbeauftragten werden keine Aufgaben übertragen, die einen Interessenkonflikt mit Aufgaben nach Absatz 2 zur Folge haben können.

Art. 83 Konferenz der Informationssicherheitsbeauftragten

[1] Die Konferenz der Informationssicherheitsbeauftragten wird aus den Informationssicherheitsbeauftragten nach Artikel 82 Absatz 1 sowie zwei Vertreterinnen oder Vertretern der Kantone und der oder dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gebildet.

[2] Sie hat folgende Aufgaben:

a. Sie fördert den einheitlichen Vollzug dieses Gesetzes.

b. Sie wirkt bei der Standardisierung der Anforderungen und Massnahmen nach Artikel 86 mit.

c. Sie berät die Fachstelle des Bundes für Informationssicherheit in allen Fragen der Vollzugskoordination und in Belangen von strategischer Bedeutung.

d. Sie sorgt für den Informationsaustausch insbesondere in Zusammenhang mit dem Risikomanagement sowie mit Problemen und Vorfällen im Bereich der Informationssicherheit.

e. Sie sorgt für die Koordination mit den anderen Stellen, die Aufgaben im Bereich der Informationssicherheit erfüllen.

[3] Die Konferenz gibt sich ein Geschäftsreglement.

Art. 84 Fachstelle des Bundes für Informationssicherheit

[1] Die Fachstelle des Bundes für Informationssicherheit hat folgende Aufgaben:

a. Sie berät und unterstützt die verpflichteten Behörden, deren Informationssicherheitsbeauftragte und die Kantone beim Vollzug dieses Gesetzes.

b. Sie kann bei Gefährdungen der Informationssicherheit des Bundes Empfehlungen abgeben.

c. Sie kann auf Antrag der verpflichteten Behörden Überprüfungen durchführen.

d. Sie kann auf Antrag der verpflichteten Behörden die Risiken für die Informationssicherheit beim Einsatz neuartiger Technologien beurteilen.

e. Sie kann auf Antrag der verpflichteten Behörden und Organisationen prüfen, ob deren Prozesse, Mittel, Einrichtungen, Gegenstände und Dienstleistungen den Anforderungen an die Informationssicherheit entsprechen.

f. Sie kann auf Antrag der verpflichteten Behörden die Informationssicherheit bei wichtigen behördenübergreifenden Projekten steuern und koordinieren.

g. Sie ist Ansprechstelle für Fachkontakte mit inländischen, ausländischen und internationalen Stellen.

h. Sie erstattet dem Bundesrat jährlich Bericht über den Stand der Informationssicherheit des Bundes.

[2] Die oder der Informationssicherheitsbeauftragte des Bundesrats ist gleichzeitig die Leiterin oder der Leiter der Fachstelle des Bundes für Informationssicherheit.

[3] Der Bundesrat regelt die Organisation der Fachstelle des Bundes für Informationssicherheit. Er kann ihr weitere Aufgaben für die Bundesverwaltung und die Armee zuweisen.

2. Abschnitt: Vollzug

Art. 85 Ausführungsbestimmungen

[1] Die verpflichteten Behörden erlassen die für den Vollzug dieses Gesetzes erforderlichen Ausführungsbestimmungen. Der Bundesrat kann den Erlass von Ausführungsbestimmungen für Bundesratsgeschäfte der Bundeskanzlei übertragen.

[2] Zuständigkeiten, die das vorliegende Gesetz den verpflichteten Behörden zuweist, werden für die Bundesversammlung durch die Verwaltungsdelegation der Bundesversammlung wahrgenommen.

[3] Die Ausführungsbestimmungen des Bundesrats gelten für die verpflichteten Behörden sinngemäss, sofern diese keine eigenen Ausführungsbestimmungen erlassen.

Art. 86 Standardanforderungen und -massnahmen

[1] Der Bundesrat legt standardisierte Sicherheitsanforderungen sowie standardisierte organisatorische, personelle, technische und bauliche Massnahmen zur Gewährleistung der Informationssicherheit nach dem Stand von Wissenschaft und Technik fest.

[2] Er kann diese Aufgabe delegieren.

[3] Die Standardanforderungen und -massnahmen haben empfehlenden Charakter, sofern sie von den verpflichteten Behörden nicht für verbindlich erklärt werden.

Art. 87 Kantone

[1] Die Kantone sorgen für die periodische Überprüfung der Umsetzung und Wirksamkeit der Informationssicherheit nach Artikel 3.

[2] Sie informieren die Fachstelle des Bundes für Informationssicherheit über die Ergebnisse der Überprüfungen nach Absatz 1.

[3] Sie bezeichnen für Fragen der Informationssicherheit je eine Dienststelle als Ansprechpartnerin für die verpflichteten Behörden.

[4] Der Bundesrat legt fest, in welchen Fällen die Kantone die Leistungen der Fachstellen nach diesem Gesetz für ihre eigene Informationssicherheit in Anspruch nehmen können. Die Leistungen sind gebührenpflichtig. Der Bundesrat legt die Höhe der Gebühren fest.

Art. 88 Völkerrechtliche Verträge

Der Bundesrat ist ermächtigt, völkerrechtliche Verträge im Bereich der Informationssicherheit abzuschliessen:

a. zum Austausch von Informationen über Gefährdungen, Schwachstellen und Vorfälle im Bereich der Informationssicherheit, insbesondere von kritischen Infrastrukturen;

b. zum Austausch von klassifizierten Informationen;

c. zur Durchführung von Personensicherheitsprüfungen und Betriebssicherheitsverfahren;

d. zur Anerkennung von Sicherheitserklärungen;

e. zur Durchführung von Kontrollen.

Art. 89 Evaluation

[1] Der Bundesrat sorgt dafür, dass die Umsetzung, die Zweckmässigkeit, die Wirksamkeit und die Wirtschaftlichkeit dieses Gesetzes periodisch überprüft werden.

[2] Er erstattet den zuständigen Kommissionen der Bundesversammlung regelmässig Bericht.

7. Kapitel: Schlussbestimmungen

Art. 90 Änderung anderer Erlasse

Die Änderung anderer Erlasse wird im Anhang geregelt.

Art. 91 Übergangsbestimmungen

[1] Nach bisherigem Recht klassifizierte Informationen werden an die Bestimmungen dieses Gesetzes angepasst, sobald sie nach Inkrafttreten dieses Gesetzes zum ersten Mal bearbeitet werden.

[2] Informatikmittel müssen innerhalb von zwei Jahren nach Inkrafttreten dieses Gesetzes eingestuft werden. Technische Massnahmen zur Gewährleistung der Informationssicherheit müssen innerhalb von sechs Jahren nach Inkrafttreten dieses Gesetzes umgesetzt werden.

[3] Nach bisherigem Recht im Rahmen von Personensicherheitsprüfungen ausgestellte Sicherheits- und Risikoerklärungen sowie nach bisherigem Recht ausgestellte Betriebssicherheitserklärungen sind fünf Jahre ab deren Ausstellung gültig.

Art. 92 Referendum und Inkrafttreten

[1] Dieses Gesetz untersteht dem fakultativen Referendum.

[2] Der Bundesrat bestimmt das Inkrafttreten.

Anhang
(Art. 90)

Änderung anderer Erlasse

Die nachstehenden Erlasse werden wie folgt geändert:

1. Bundesgesetz vom 21. März 1997[21] über Massnahmen zur Wahrung der inneren Sicherheit

Art. 2 Abs. 4 Bst. c

Aufgehoben

4. Abschnitt (Art. 19–21)

Aufgehoben

Art. 24a Abs. 7 erster Satz

[7] Das Informationssystem steht den für den Vollzug dieses Gesetzes zuständigen Stellen von fedpol sowie den Polizeibehörden der Kantone, der Schweizerischen Zentralstelle für Hooliganismus (Zentralstelle), den Zollbehörden und den für die Durchführung der Personensicherheitsprüfungen zuständigen Fachstellen nach Artikel 32 Absatz 2 des Informationssicherheitsgesetzes vom ... [22] über ein Abrufverfahren zur Verfügung. …

2. Nachrichtendienstgesetz vom 25. September 2015[23]

Art. 51 Abs. 4 Bst. d

[4] Die folgenden Personen haben im Abrufverfahren Zugriff auf die nachstehenden Daten in INDEX NDB:

d. die Mitarbeiterinnen und Mitarbeiter der für die Durchführung der Personensicherheitsprüfungen zuständigen Fachstellen nach Artikel 32 Absatz 2 des Informationssicherheitsgesetzes vom ... [24] auf die Daten nach Absatz 3 Buchstabe a zur Durchführung von Personensicherheitsprüfungen und von

21 SR **120**
22 SR ...
23 BBl **2015** 7211
24 SR ...

Prüfungen der Vertrauenswürdigkeit sowie zur Beurteilung des Gewaltpotenzials.

3. Bundespersonalgesetz vom 24. März 2000[25]

Art. 20a Auszug aus dem Strafregister und dem Betreibungsregister

Die Arbeitgeber können von Stellenbewerberinnen und Stellenbewerbern sowie von ihren Angestellten verlangen, dass sie einen Auszug aus dem Strafregister und aus dem Betreibungsregister vorlegen, sofern dies zur Wahrung der Interessen des Arbeitgebers erforderlich ist.

Art. 20b Prüfung der Vertrauenswürdigkeit

[1] Die Arbeitgeber nach Artikel 3 Absatz 1 Buchstaben a, b, e und f können Stellenbewerberinnen und Stellenbewerber sowie ihre Angestellten auf deren Vertrauenswürdigkeit hin prüfen lassen, wenn diese im Rahmen ihrer Funktion:

a. die Schweiz im Ausland regelmässig vertreten sollen und dabei das Ansehen des Bundes erheblich beeinträchtigen könnten;

b. in wesentlichen Finanz- oder Steuersachen Entscheide fällen oder Aufsichtsaufgaben wahrnehmen sollen und dabei die finanziellen Interessen des Bundes erheblich beeinträchtigen könnten.

[2] Sie beschränken sich bei der Prüfung auf das erforderliche Mindestmass.

[3] Die Vertrauenswürdigkeitsprüfungen werden von den Fachstellen nach Artikel 32 Absatz 2 des Informationssicherheitsgesetzes vom ...[26] (ISG) durchgeführt. Das Verfahren richtet sich sinngemäss nach den entsprechenden Bestimmungen des ISG.

[4] Werden die Stellenbewerberinnen und Stellenbewerber sowie die Angestellten gleichzeitig einer Personensicherheitsprüfung nach dem ISG unterzogen, so werden die beiden Verfahren vereinigt.

25 SR **172.220.1**
26 SR ...

4. Zivilprozessordnung[27]

Art. 166 Abs. 1 Bst. c

[1] Eine dritte Person kann die Mitwirkung verweigern:

c. zur Feststellung von Tatsachen, die ihr als Beamtin oder Beamter im Sinne von Artikel 110 Absatz 3 StGB oder als Behördenmitglied in ihrer amtlichen Eigenschaft anvertraut worden sind oder die sie bei Ausübung ihres Amtes oder bei Ausübung ihrer Hilfstätigkeit für eine Beamtin oder einen Beamten oder eine Behörde wahrgenommen hat; sie hat auszusagen, wenn sie einer Anzeigepflicht unterliegt oder wenn sie von ihrer vorgesetzten Behörde zur Aussage ermächtigt worden ist;

5. Bundesgesetz vom 4. Dezember 1947[28] über den Bundeszivilprozess

Art. 42 Abs. 3

[3] Für die Zeugnispflicht von Beamten und deren Hilfspersonen über Wahrnehmungen in Ausübung ihres Amtes oder ihrer Hilfstätigkeit sind die einschränkenden Vorschriften des Verwaltungsrechtes des Bundes und der Kantone massgebend.

6. Strafgesetzbuch[29]

Art. 320 Verletzung des Amtsgeheimnisses

1. Wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist oder das er in seiner amtlichen oder dienstlichen Stellung oder als Hilfsperson eines Beamten oder einer Behörde wahrgenommen hat, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Die Verletzung des Amtsgeheimnisses ist auch nach Beendigung des amtlichen oder dienstlichen Verhältnisses oder der Hilfstätigkeit strafbar.

2. Der Täter ist nicht strafbar, wenn er das Geheimnis mit schriftlicher Einwilligung seiner vorgesetzten Behörde geoffenbart hat.

27 SR **272**
28 SR **273**
29 SR **311.0**

Art. 365 Abs. 2 Bst. d

[2] Das Register dient der Unterstützung von Behörden des Bundes und der Kantone bei der Erfüllung folgender Aufgaben:

d. Beurteilung des Sicherheitsrisikos im Rahmen der Personensicherheitsprüfungen nach dem Informationssicherheitsgesetz vom ...[30] (ISG) und im Rahmen der Prüfungen der Vertrauenswürdigkeit nach der Spezialgesetzgebung;

Art. 367 Abs. 2 Bst. i, Abs. 2bis Bst. b und Abs. 4

[2] Folgende Behörden dürfen durch ein Abrufverfahren Einsicht in die Personendaten über Urteile nach Artikel 366 Absätze 1, 2 und 3 Buchstaben a und b nehmen:

i. die für die Durchführung der Personensicherheitsprüfungen zuständigen Fachstellen nach Artikel 32 Absatz 2 ISG[31] (Fachstellen PSP);

[2bis] Folgende Behörden dürfen durch ein Abrufverfahren auch Einsicht in die Personendaten über Urteile nach Artikel 366 Absatz 3 Buchstabe c nehmen:

b. die Fachstellen PSP;

[4] Personendaten über hängige Strafverfahren dürfen nur durch die Behörden nach Absatz 2 Buchstaben a–e, i, j und l bearbeitet werden.

7. Strafprozessordnung[32]

Art. 170 Abs. 1

[1] Beamtinnen und Beamte im Sinne von Artikel 110 Absatz 3 StGB[33] und ihre Hilfspersonen sowie Mitglieder von Behörden und ihre Hilfspersonen können das Zeugnis über Geheimnisse verweigern, die ihnen in ihrer amtlichen Eigenschaft anvertraut worden sind oder die sie bei der Ausübung ihres Amtes oder ihrer Hilfstätigkeit wahrgenommen haben.

30 SR ...
31 SR ...
32 SR **312.0**
33 SR **311.0**

8. Militärstrafgesetz vom 13. Juni 1927[34]

Art. 77 Verletzung des Dienstgeheimnisses

1. Wer ein Geheimnis offenbart, das ihm in dienstlicher oder amtlicher Eigenschaft anvertraut wird oder das er in seiner dienstlichen oder amtlichen Stellung oder als Hilfsperson eines solchen Geheimnisträgers wahrnimmt, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

In leichten Fällen erfolgt disziplinarische Bestrafung.

2. Die Verletzung des Dienst- oder Amtsgeheimnisses ist auch nach Beendigung des dienstlichen oder amtlichen Verhältnisses oder der Hilfstätigkeit strafbar.

9. Militärstrafprozess vom 23. März 1979[35]

Art. 77 Abs. 2

[2] Ein Beamter oder seine Hilfsperson darf nur mit Zustimmung der vorgesetzten Behörde über ein Amtsgeheimnis (Art. 320 StGB[36]) als Zeuge einvernommen oder zur Herausgabe von Amtsakten angehalten werden. Im Übrigen gelten das eidgenössische und das kantonale Verwaltungsrecht.

10. Bundesgesetz vom 13. Juni 2008[37] über die polizeilichen Informationssysteme des Bundes

Art. 15 Abs. 4 Bst. f

Aufgehoben

Art. 17 Abs. 4 Einleitungssatz und Bst. l

[4] Zugriff auf diese Daten mittels Abrufverfahren haben:

l. die für die Durchführung der Personensicherheitsprüfungen zuständigen Fachstellen nach Artikel 32 Absatz 2 des Informationssicherheitsgesetzes vom ... [38] zur Beurteilung des Sicherheitsrisikos im Rahmen einer Personensicherheitsprüfung, einer Prüfung der Vertrauenswürdigkeit oder einer Beurteilung des Gewaltpotenzials.

34 SR **321.0**
35 SR **322.1**
36 SR **311.0**
37 SR **361**
38 SR ...

11. Militärgesetz vom 3. Februar 1995[39]

Art. 14 Prüfung der Vertrauenswürdigkeit

[1] Die Angehörigen der Armee können auf ihre Vertrauenswürdigkeit hin geprüft werden, wenn sie im Rahmen ihrer Funktion:

a. die Schweiz im Ausland regelmässig vertreten sollen und dabei das Ansehen des Bundes erheblich beeinträchtigen könnten;

b. in wesentlichen finanziellen Angelegenheiten Entscheide fällen oder Aufsichtsaufgaben wahrnehmen sollen und dabei die finanziellen Interessen des Bundes erheblich beeinträchtigen könnten.

[2] Der Bundesrat legt fest, welche Funktionen geprüft werden müssen. Er beschränkt sich dabei auf das erforderliche Mindestmass.

[3] Die Vertrauenswürdigkeitsprüfungen werden von der Fachstelle nach Artikel 32 Absatz 2 des Informationssicherheitsgesetzes vom ...[40] (ISG) durchgeführt. Das Verfahren richtet sich sinngemäss nach den entsprechenden Bestimmungen des ISG.

[4] Werden die Angehörigen der Armee gleichzeitig einer Personensicherheitsprüfung nach dem ISG unterzogen, so werden die beiden Verfahren vereinigt.

Art. 113 Abs. 6

[6] Das Verfahren richtet sich sinngemäss nach den Bestimmungen über die Grundsicherheitsprüfung nach Artikel 31 Buchstabe a ISG[41]. Ist gleichzeitig aus anderen Gründen eine Grundsicherheitsprüfung durchzuführen, so werden die beiden Verfahren vereinigt.

Art. 150 Abs. 4

Aufgehoben

12. Bundesgesetz vom 3. Oktober 2008[42] über die militärischen Informationssysteme

Art. 14 Abs. 1 Bst. i

[1] Das PISA enthält folgende Daten der Stellungspflichtigen, der Militärdienstpflichtigen, des für die Friedensförderung vorgesehenen Personals sowie von Zivilperso-

39 SR **510.10**
40 SR ...
41 SR ...
42 SR **510.91**

nen, die von der Truppe betreut oder für einen befristeten Einsatz der Armee beigezogen werden:

i. Daten über die Durchführung der Prüfung der Vertrauenswürdigkeit nach Artikel 14 des Militärgesetzes vom 3. Februar 1995[43] (MG), mit Entscheid.

Art. 17 Abs. 1 Bst. a

[1] Daten des PISA über Straftaten sowie strafrechtliche Entscheide und Massnahmen dürfen nur aufbewahrt werden, wenn gestützt auf diese Daten:

a. ein Entscheid über die Nichtrekrutierung, den Ausschluss oder die Degradation nach dem MG[44] erging;

5. Kapitel 1. und 2. Abschnitt (Artikel 144–155)

Aufgehoben

13. Kernenergiegesetz vom 21. März 2003[45]

Art. 5 Abs. 3 und Abs. 3bis

[3] Um zu verhindern, dass die nukleare Sicherheit von Kernanlagen und Kernmaterialien durch unbefugtes Einwirken beeinträchtigt oder Kernmaterialien entwendet werden, müssen Sicherungsmassnahmen getroffen werden.

[3bis] Die Klassifizierung und Bearbeitung von Informationen richten sich nach den Vorschriften der Gesetzgebung über die Informationssicherheit beim Bund.

14. Stromversorgungsgesetz vom 23. März 2007[46]

Art. 20a Prüfung der Vertrauenswürdigkeit

[1] Angestellte der nationalen Netzgesellschaft, die Aufgaben erfüllen sollen, die für die Sicherheit des Übertragungsnetzes auf gesamtschweizerischer Ebene und dessen zuverlässigen und leistungsfähigen Betrieb wesentlich sind, werden zur Beurteilung des Sicherheitsrisikos auf ihre Vertrauenswürdigkeit hin geprüft.

[2] Der Bundesrat legt fest, welche Personengruppen geprüft werden müssen. Er beschränkt sich dabei auf das erforderliche Mindestmass.

43 SR **510.10**
44 SR **510.10**
45 SR **732.1**
46 SR **734.7**

[3] Die Vertrauenswürdigkeitsprüfungen werden von der Fachstelle nach Artikel 32 Absatz 2 des Informationssicherheitsgesetzes vom ...[47] (ISG) durchgeführt. Das Verfahren richtet sich sinngemäss nach den entsprechenden Bestimmungen des ISG.

[4] Die Ergebnisse der Prüfung werden der Geschäftsleitung der nationalen Netzgesellschaft, dem Bundesamt und der ElCom mitgeteilt.

15. Nationalbankgesetz vom 3. Oktober 2003[48]

Art. 16 Sachüberschrift und Abs. 5

Vertraulichkeit und Informationssicherheit

[5] Im Übrigen gelten die Bestimmungen des Bundesgesetzes vom 19. Juni 1992[49] über den Datenschutz sowie des Informationssicherheitsgesetzes vom...[50].

47 SR ...
48 SR **951.11**
49 **SR 235.1**
50 SR ...