Bundesgesetz über die Informationssicherheit (ISG)

vom …

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 den sicheren Umgang mit Informationen sowie den sicheren Einsatz von Informations- und Kommunikationstechnologien gewährleisten.

[2] Es soll damit die folgenden öffentlichen Interessen schützen:

a. die Entscheidungs- und Handlungsfähigkeit der Bundesbehörden;
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 Bundesbehörden 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;
c. die eidgenössischen Gerichte;

AS **...**

1 SR **101**
2 BBl **...**

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 des öffentlichen und privaten Rechts, die im Rahmen der Erfüllung von Verwaltungsaufgaben im Sinne von Artikel 2 Absatz 4 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[3] sicherheitsempfindliche Tätigkeiten ausüben;

f. kantonale Behörden und Stellen, die im Auftrag des Bundes und unter seiner Aufsicht sicherheitsempfindliche Tätigkeiten ausüben.

[3] Als sicherheitsempfindliche Tätigkeiten gelten:

a. die Bearbeitung von als «VERTRAULICH» oder «GEHEIM» klassifizierten Informationen oder der Umgang mit entsprechend klassifiziertem Material (Art. 14 Abs. 2 und 3);

b. die Verwaltung, der Betrieb, die Wartung oder die Überprüfung von IKT-Mitteln der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz» (Art. 21 Abs. 2 und 3);

c. der Zugang zu Sicherheitszonen, insbesondere zu Schutzzonen 2 oder 3 einer Anlage nach der Gesetzgebung über den Schutz militärischer Anlagen (Art. 31).

Art. 3 Verhältnis zur Spezialgesetzgebung

[1] Das Öffentlichkeitsgesetz vom 17. Dezember 2004[4] bleibt vorbehalten.

[2] Soweit Informationen aufgrund anderer Bundesgesetze geschützt werden müssen, finden die Bestimmungen des vorliegenden Gesetzes ergänzend Anwendung.

[3] Die Anwendung des vorliegenden Gesetzes auf Organisationen des öffentlichen und privaten Rechts, die Infrastrukturen betreiben, die für das Funktionieren von Gesellschaft, Wirtschaft und Staat unerlässlich sind (kritische Infrastrukturen), richtet sich nach der Spezialgesetzgebung.

3 SR **172.010**
4 SR **152.3**

2. Kapitel: Allgemeine Massnahmen der Informationssicherheit

1. Abschnitt: Grundsätze

Art. 4 Informationssicherheit

[1] Die verpflichteten Behörden und Organisationen sorgen dafür, dass der Schutzbedarf der Informationen, für die sie zuständig sind, im Hinblick auf eine allfällige 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).

[3] Sie sorgen dafür, dass die Mittel der Informations- und Kommunikationstechnologien (IKT-Mittel), die sie zur Erfüllung ihrer gesetzlichen Aufgaben einsetzen, vor Missbrauch und vor Störung geschützt werden.

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

Art. 5 Oberste Führungsverantwortung

[1] Die verpflichteten Behörden sorgen in ihrem Zuständigkeitsbereich dafür, dass:

a. die Informationssicherheit nach dem Stand der Lehre und Technik organisiert, umgesetzt und überprüft wird;

b. die Informationssicherheit unter den Fachbereichen koordiniert wird.

[2] Sie legen die Aufgaben der betroffenen Stellen fest.

[3] Sie legen ferner fest:

a. ihre Ziele für die Informationssicherheit;

b. die Eckwerte für den Umgang mit Risiken;

c. die Folgen bei Missachtung der Vorschriften.

[4] Sie sorgen dafür, dass die Führungskräfte und das Personal regelmässig und stufengerecht informiert werden.

Art. 6 Risikomanagement

[1] Die verpflichteten Behörden und Organisationen sorgen dafür, dass die Risiken für die Informationssicherheit in ihrem Zuständigkeitsbereich sowie bei der Zusammenarbeit mit Dritten laufend identifiziert, bewertet, beurteilt und überprüft werden.

[2] Sie sorgen dafür, dass die erforderlichen organisatorischen, personellen, technischen und baulichen Massnahmen getroffen werden, um die identifizierten Risiken zu vermeiden oder sie auf ein tragbares Mass zu reduzieren.

[3] Sie sorgen dafür, dass Risiken, die getragen werden sollen, nachweislich kommuniziert und akzeptiert werden.

[4] Das Risikomanagement im Bereich der Informationssicherheit muss in den allgemeinen Risikomanagementprozess integriert werden.

Art. 7 Sicherheitsanforderungen und -massnahmen

[1] Die verpflichteten Behörden und Organisationen orientieren sich bei der Festlegung der Sicherheitsanforderungen und -massnahmen an den Standardanforderungen und -massnahmen nach Artikel 88.

[2] Die Sicherheitsmassnahmen richten sich nach dem Stand der Lehre und der Technik.

Art. 8 Zusammenarbeit mit Dritten

[1] Die verpflichteten Behörden und Organisationen sorgen dafür, dass bei der Zusammenarbeit mit Dritten die Anforderungen und Massnahmen nach diesem Gesetz in den entsprechenden Vereinbarungen und Verträgen festgelegt werden.

[2] Sie überprüfen die Umsetzung der Massnahmen.

Art. 9 Vorgehen bei Verletzungen der Informationssicherheit

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

Art. 10 Vorsorgeplanungen

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

Art. 11 Kontrollen

[1] Die verpflichteten Behörden und Organisationen sorgen dafür, dass die Einhaltung der Vorschriften dieses Gesetzes regelmässig überprüft wird.

[2] Die verpflichteten Behörden lassen periodisch die Wirksamkeit der getroffenen Massnahmen in ihrem Zuständigkeitsbereich durch eine unabhängige Stelle prüfen.

2. Abschnitt: Klassifizierung von Informationen

Art. 12 Grundsätze der Klassifizierung

[1] Die verpflichteten Behörden und Organisationen sorgen dafür, dass Informationen, welche die Kriterien von Artikel 14 erfüllen, entsprechend klassifiziert werden.

[2] Die Klassifizierung ist auf das notwendige Mindestmass zu beschränken.

[3] Sie ist zeitlich zu begrenzen, wenn voraussehbar ist, dass sie nur bis zu einem bestimmten Zeitpunkt erforderlich ist.

[4] Jede Klassifizierung muss periodisch überprüft werden.

Art. 13 Zuständigkeiten

[1] Die verpflichteten Behörden legen fest, welche Personen oder Stellen für die Klassifizierung der Informationen zuständig sind (klassifizierende Stelle).

[2] Klassifizierungen dürfen nur von der klassifizierenden Stelle oder von der ihr vorgesetzten Stelle geändert oder aufgehoben werden.

Art. 14 Klassifizierungsstufen

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

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

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

Art. 15 Zugang zu klassifizierten Informationen

[1] Zugang zu klassifizierten Informationen des Bundes erhalten nur Personen, die Gewähr dafür bieten, dass sie mit klassifizierten Informationen 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] Vorbehalten bleiben durch völkerrechtliche Verträge nach Artikel 90 geregelte Zugangsbeschränkungen.

Art. 16 Bearbeitung von klassifizierten Informationen

[1] Klassifizierte Informationen müssen während der ganzen Dauer ihrer Schutzwürdigkeit vor unberechtigter Kenntnisnahme geschützt werden.

[2] Sie müssen einen Hinweis auf die klassifizierende Stelle enthalten.

[3] Die Bearbeitung klassifizierter Informationen aus dem Ausland richtet sich nach dem entsprechenden völkerrechtlichen Vertrag nach Artikel 90.

Art. 17 Bekanntgabe klassifizierter Informationen in besonderen Verfahren

[1] Die Bekanntgabe klassifizierter Informationen in der Bundesversammlung, in den Parlamentsdiensten sowie in den Gerichten und Staatsanwaltschaften richtet sich nach dem jeweils anwendbaren Verfahrensrecht.

[2] Vor dem Entscheid, eine Information nach Absatz 1 bekannt zu geben, kann das zuständige parlamentarische Organ oder das zuständige Gericht die klassifizierende Stelle anhören.

Art. 18 Vorläufige Schutzmassnahmen

[1] Verpflichtete Behörden und Organisationen sorgen dafür, dass der klassifizierenden Stelle Meldung erstattet wird, wenn:

a. klassifizierte Informationen gefährdet oder missbraucht werden oder verloren gegangen sind;

b. Informationen offensichtlich falsch klassifiziert oder fälschlicherweise nicht klassifiziert sind.

[2] Sie treffen die erforderlichen Massnahmen, um die betreffenden Informationen vorläufig zu schützen.

3. Abschnitt: Sicherheit beim Einsatz von IKT-Mitteln

Art. 19 Sicherheitsverfahren

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

[2] Für die Durchführung des Sicherheitsverfahrens ist die verpflichtete Behörde oder Organisation zuständig, die zur Erfüllung ihrer gesetzlichen Aufgaben den Betrieb von IKT-Mitteln in Auftrag gibt oder selbst IKT-Mittel betreibt.

[3] Das Sicherheitsverfahren muss bei Veränderung der Risiken wiederholt werden.

Art. 20 Schutzbedarfsanalyse und Risikobeurteilung

[1] Die verpflichteten Behörden und Organisationen sorgen dafür, dass die Bedürfnisse der Informationssicherheit bei der Planung des Einsatzes von IKT-Mitteln beurteilt werden.

[2] Die verpflichteten Behörden und Organisationen, die neuartige Technologien einsetzen wollen, sorgen für eine Beurteilung der Risiken für die Informationssi-

cherheit, die damit verbunden sind. Sie teilen die Risikobeurteilung der Fachstelle des Bundes für Informationssicherheit mit.

Art. 21 Sicherheitseinstufung von IKT-Mitteln

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

[2] Die Sicherheitsstufe «hoher Schutz» gilt für IKT-Mittel:

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

b. deren Störung oder Missbrauch die Interessen nach Artikel 1 Absatz 2 erheblich beeinträchtigen kann.

[3] Die Sicherheitsstufe «sehr hoher Schutz» gilt für IKT-Mittel:

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

b. deren Störung oder Missbrauch die Interessen nach Artikel 1 Absatz 2 schwerwiegend beeinträchtigen kann.

Art. 22 Sicherheitsanforderungen der Sicherheitsstufe «Grundschutz»

[1] Die verpflichteten Behörden legen die Mindestanforderungen für IKT-Mittel der Sicherheitsstufe «Grundschutz» fest.

[2] Diese Mindestanforderungen müssen für sämtliche IKT-Mittel erfüllt werden.

Art. 23 Informationssicherheitskonzept

[1] Die verpflichteten Behörden und Organisationen sorgen dafür, dass für IKT-Mittel der Sicherheitsstufen «hoher Schutz» und «sehr hoher Schutz» eine Risikoanalyse durchgeführt und ein Informationssicherheitskonzept erstellt wird.

[2] Das Informationssicherheitskonzept muss durch die zuständige Informationssicherheitsbeauftragte oder den zuständigen Informationssicherheitsbeauftragten geprüft werden und von der verpflichteten Behörde oder Organisation genehmigt werden.

[3] Es muss laufend aktualisiert werden.

Art. 24 Konformitäts- und Wirksamkeitsprüfungen

[1] Bevor ein IKT-Mittel eingesetzt werden darf, muss geprüft werden, ob das Sicherheitsverfahren rechtmässig durchgeführt wurde und die beschlossenen Massnahmen umgesetzt wurden.

[2] Bevor ein IKT-Mittel der Sicherheitsstufe «sehr hoher Schutz» eingesetzt werden darf, muss zudem die Wirksamkeit der umgesetzten Massnahmen geprüft werden.

Art. 25 Sicherheitsfreigabe

[1] Die verpflichteten Behörden und Organisationen geben nach Durchführung des Sicherheitsverfahrens das IKT-Mittel für den Einsatz frei.

[2] Mit der Sicherheitsfreigabe akzeptiert die Behörde oder Organisation die Restrisiken.

Art. 26 Inventar der IKT-Mittel

Die verpflichteten Behörden und Organisationen sorgen dafür, dass ihre IKT-Mittel inventarisiert werden.

Art. 27 Sicherheit beim Betrieb

Die verpflichteten Behörden und Organisationen, die IKT-Mittel betreiben, sorgen dafür, dass die Informationssicherheit beim Betrieb dieser Mittel gewährleistet wird.

4. Abschnitt: Personelle Massnahmen

Art. 28 Personelle Anforderungen beim Umgang mit Informationen und IKT-Mitteln des Bundes

Die verpflichteten Behörden und Organisationen sorgen dafür, dass Personen, die im Rahmen ihrer Aufgaben oder eines Auftrags mit Informationen oder IKT-Mitteln des Bundes umgehen sollen:

a. sorgfältig ausgewählt werden;

b. stufengerecht aus- und weitergebildet werden;

c. gegebenenfalls zur Geheimhaltung verpflichtet werden.

Art. 29 Restriktive Erteilung von Berechtigungen

[1] Die verpflichteten Behörden und Organisationen sorgen dafür, dass nur diejenigen Berechtigungen für den Umgang mit Informationen und IKT-Mitteln sowie für den Zugang zu Räumlichkeiten erteilt werden, welche die betreffenden Personen zur Erfüllung ihrer Aufgaben benötigen.

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

[3] Die verpflichteten Behörden und Organisationen sorgen für die regelmässige Überprüfung der Berechtigungen.

5. Abschnitt: Physischer Schutz von Informationen und IKT-Mitteln

Art. 30 Grundsätze

[1] Die verpflichteten Behörden und Organisationen sorgen in ihren Räumlichkeiten für einen angemessen physischen Schutz ihrer Informationen und IKT-Mittel vor unberechtigtem Zugang sowie vor Beschädigung und Störung.

[2] Sie sorgen dafür, dass Informationen und IKT-Mittel in öffentlich zugänglichen Bereichen angemessen geschützt werden.

Art. 31 Sicherheitszonen

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

a. häufig als «VERTRAULICH» oder «GEHEIM» klassifizierte Informationen bearbeitet werden; oder

b. IKT-Mittel der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz» betrieben werden.

[2] Sie sorgen dafür, dass nur identifizierte und berechtigte Personen Zutritt zu den Sicherheitszonen erhalten.

[3] Soweit dies zur Gewährleistung der Informationssicherheit erforderlich ist, sind die verpflichteten Behörden und Organisationen befugt, in Sicherheitszonen:

a. biometrische Verifikationsmethoden zu verwenden;

b. die Mitnahme bestimmter Gegenstände, insbesondere von Aufnahmegeräten, zu verbieten;

c. sicherheitsempfindliche Bereiche mit technischen Aufnahmegeräten zu überwachen;

d. Taschen- und Personenkontrollen durchzuführen;

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

[4] Sie sind ferner befugt, in Sicherheitszonen, in welchen als «GEHEIM» klassifizierte Informationen häufig bearbeitet werden oder IKT-Mittel der Sicherheitsstufe «sehr hoher Schutz» betrieben werden, störende Fernmeldeanlagen nach Artikel 34 Absatz 1[ter] des Fernmeldegesetzes vom 30. April 1997[5] zu betreiben.

[5] Vorbehalten bleiben die besonderen Vorschriften für Sicherheitszonen gemäss völkerrechtlichen Verträgen nach Artikel 90 sowie die Vorschriften für Schutzzonen von Anlagen nach der Gesetzgebung über den Schutz militärischer Anlagen.

5 SR **784.10**

3. Kapitel: Personensicherheitsprüfung

1. Abschnitt: Prüfzweck, zu prüfende Personen und Prüfstufen

Art. 32 Prüfzweck

Mit der Personensicherheitsprüfung wird beurteilt, ob ein Sicherheitsrisiko besteht, wenn eine Person im Rahmen ihrer Funktion oder eines Auftrags eine sicherheitsempfindliche Tätigkeit ausüben soll.

Art. 33 Liste der Funktionen mit sicherheitsempfindlicher Tätigkeit

Die verpflichteten Behörden erlassen für ihren Zuständigkeitsbereich eine Liste der Funktionen, für deren Aufgabenerfüllung die Ausübung einer sicherheitsempfindlichen Tätigkeit erforderlich ist.

Art. 34 Zu prüfende Personen

[1] Eine Personensicherheitsprüfung wird bei Personen durchgeführt:

a. die eine Funktion ausüben sollen, die in einer Liste nach Artikel 33 enthalten ist;

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

c. die aufgrund eines völkerrechtlichen Vertrags nach Artikel 90 einer Personensicherheitsprüfung unterzogen werden müssen.

[2] Soll eine Person von einer ausländischen oder internationalen Behörde mit der Ausübung einer sicherheitsempfindlichen Tätigkeit betraut werden, so wird die Personensicherheitsprüfung durchgeführt, sofern die Schweiz mit dem betreffenden Land oder der betreffenden internationalen Organisation einen völkerrechtlichen Vertrag nach Artikel 90 abgeschlossen hat.

[3] Bei Personen, die eine Funktion ausüben oder ausüben sollen, die in einer Liste nach Artikel 33 enthalten sein müsste, aber noch nicht darin aufgenommen wurde, kann mit Zustimmung der verpflichteten Behörde eine Personensicherheitsprüfung durchgeführt werden. Die Funktionenliste muss bei nächster Gelegenheit angepasst werden.

[4] Keiner Personensicherheitsprüfung unterstehen in ihrer Eigenschaft als Behördenmitglieder:

a. die Mitglieder der Bundesversammlung;

b. die Mitglieder des Bundesrates und der Bundeskanzler bzw. die Bundeskanzlerin;

c. die Richterinnen und die Richter der eidgenössischen Gerichte;

d. die Bundesanwältin oder der Bundesanwalt;

e. die Mitglieder der Aufsichtsbehörde über die Bundesanwaltschaft;

f. die Mitglieder der kantonalen Regierungen und Gerichte.

Art. 35 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. 36 Einleitende Stellen

Die verpflichteten Behörden legen fest, welche Stellen für die Einleitung der Personensicherheitsprüfungen zuständig sind (einleitende Stellen).

Art. 37 Einwilligung

[1] Eine Personensicherheitsprüfung darf nur mit der Einwilligung der zu prüfenden Person durchgeführt werden.

[2] Personensicherheitsprüfungen für Funktionen der Armee und des Zivilschutzes dürfen ohne Einwilligung der zu prüfenden Personen durchgeführt werden.

Art. 38 Zeitpunkt der Personensicherheitsprüfung

[1] Bei Personen nach Artikel 34 Absatz 1 Buchstabe a muss die Personensicherheitsprüfung eingeleitet werden, bevor die Funktion übertragen wird.

[2] Bei Personen nach Artikel 34 Absatz 1 Buchstabe a, die dem Bundesrat zur Wahl vorgeschlagen werden, muss die Personensicherheitsprüfung abgeschlossen sein, bevor die Person zur Wahl vorgeschlagen wird.

[3] Bei Personen nach Artikel 34 Absatz 1 Buchstabe b muss die Personensicherheitsprüfung abgeschlossen sein, bevor sie mit der Ausübung der sicherheitsempfindlichen Tätigkeit betraut werden.

[4] Der Zeitpunkt der Personensicherheitsprüfung bei Personen, die aufgrund völkerrechtlicher Verträge nach Artikel 90 geprüft werden müssen, richtet sich nach den Bestimmungen des entsprechenden Vertrags.

Art. 39 Datenerhebung

[1] Die für die Beurteilung des Sicherheitsrisikos zuständigen Fachstellen für Personensicherheitsprüfungen (Fachstellen PSP) können für die Grundsicherheitsprüfung Daten über die zu prüfende Person erheben:

a. aus dem Strafregister;

b. bei den zuständigen Strafverfolgungsorganen und Gerichten über laufende, abgeschlossene oder eingestellte Strafverfahren sowie die sich darauf beziehenden Gerichts- und Untersuchungsakten;

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

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

e. aus den Registern der Betreibungs- und Konkursbehörden;

f. aus den Akten bereits erfolgter Personensicherheitsprüfungen;

g. aus öffentlich zugänglichen Quellen.

[2] Die Fachstellen PSP können für die erweiterte Personensicherheitsprüfung zudem Daten über die zu prüfende Person 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] Die Fachstellen PSP können ausländische Dienststellen um die Zustellung von Daten ersuchen, die den Daten nach den Absätzen 1 und 2 entsprechen.

[4] Für die Beurteilung des Sicherheitsrisikos müssen die Fachstellen PSP auf genügend Daten über einen hinreichenden Zeitraum zurückgreifen können.

[5] Ergibt die Datenerhebung Hinweise auf einen sicherheitsrelevanten Umstand oder sind für die Beurteilung nicht genügend Daten über einen hinreichenden Zeitraum vorhanden, so können die Fachstellen PSP die zu prüfende Person dazu befragen. Sie können mit der Einwilligung der zu prüfenden Person auch Dritte befragen; diese sind nicht zur Auskunft verpflichtet.

[6] Daten über Dritte, die untrennbar mit den Daten über die zu prüfende Person verbunden sind, dürfen bearbeitet werden, sofern dies für die Beurteilung des Sicherheitsrisikos unerlässlich ist. Die Fachstellen PSP informieren die betroffenen Dritten über die Bearbeitung.

Art. 40 Kostentragung

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

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

Art. 41 Einstellung

[1] Die Fachstellen PSP stellen das Prüfverfahren ein, wenn:

a. die zu prüfende Person ihre Einwilligung zurückzieht oder an der Prüfung nicht mitwirkt;

b. die zu prüfende Person aus einem anderen Grund nicht mehr für die Funktion oder den Auftrag in Frage kommt.

[2] Die Fachstellen PSP teilen die Einstellung des Prüfverfahrens der zu prüfenden Person und der einleitenden Stelle mit. Die zu prüfende Person gilt damit als nicht geprüft.

[3] Wird das Prüfverfahren eingestellt, so werden alle bereits erhobenen Daten und Akten vernichtet.

3. Abschnitt: Beurteilung des Sicherheitsrisikos

Art. 42 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 Hinweise auf folgende persönliche Eigenschaften vorliegen:

a. mangelnde persönliche Integrität oder Vertrauenswürdigkeit;

b. Erpressbarkeit oder Bestechlichkeit; oder

c. beeinträchtigtes Beurteilungs- oder Entscheidungsvermögen.

[3] Das Sicherheitsrisiko muss ungeachtet des Verschuldens der geprüften Person durch die tatsächlichen Umstände ihrer persönlichen Verhältnisse begründet werden.

[4] Für die Beurteilung des Sicherheitsrisikos sind die Fachstellen PSP weisungsungebunden.

Art. 43 Ergebnis der Beurteilung

[1] Die Fachstellen PSP stellen eine der folgenden Erklärungen aus:

a. Sicherheitserklärung: Es besteht kein Sicherheitsrisiko.

b. Sicherheitserklärung mit Vorbehalt: Es besteht ein Sicherheitsrisiko, das aber mit Auflagen hinreichend reduziert werden kann. Die Fachstellen PSP empfehlen 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 Fachstellen PSP eine Erklärung nach Absatz 1 Buchstaben b-d ausstellen, geben sie der geprüften Person Gelegenheit zur Stellungnahme.

Art. 44 Mitteilung der Beurteilung

[1] Die Fachstellen PSP teilen ihre Erklärung der geprüften Person sowie der für die Übertragung der sicherheitsempfindlichen Tätigkeit zuständigen Stelle (übertragenden Stelle) schriftlich mit.

[2] Bei den vom Bundesrat zu wählenden Personen teilen die Fachstellen PSP dem antragstellenden Departement ihre Erklärungen zuhanden des Bundesrats mit.

[3] Die Fachstellen PSP können die jeweiligen übertragenden Stellen über das Ergebnis der Beurteilung informieren, wenn die geprüfte Person:

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

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

c. als Angehörige der Armee einer Prüfung des Gewaltpotenzials nach Artikel 113 des Militärgesetzes vom 3. Februar 1995[6] (MG) untersteht.

[4] Die Fachstellen PSP können zudem die nach Artikel 113 MG für das Überlassen oder den Entzug der persönlichen Armeewaffe zuständige Stelle über das Ergebnis der Beurteilung informieren.

Art. 45 Mitteilung von Erkenntnissen vor Abschluss der Personensicherheitsprüfung

Haben die Fachstellen PSP bereits vor Abschluss der Beurteilung konkrete Anhaltspunkte, dass ein Sicherheitsrisiko bestehen könnte, und ist die Sache dringlich, so können sie die Behörden oder Stellen nach Artikel 44 sowie die zu prüfende Person schriftlich über die bisherigen Erkenntnisse informieren.

6 SR **510.10**

4. Abschnitt: Folgen der Beurteilung

Art. 46 Ausübung der sicherheitsempfindlichen Tätigkeit

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

[2] Die übertragende Stelle entscheidet nach Kenntnisnahme der Beurteilung, ob die geprüfte Person die sicherheitsempfindliche Tätigkeit ausüben darf.

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

Art. 47 Mitteilungspflicht

Die übertragende Stelle teilt der zuständigen Fachstelle PSP schriftlich mit, wenn sie:

a. die Ausübung der sicherheitsempfindlichen Tätigkeit einer Person überträgt, für die eine Erklärung nach Artikel 43 Absatz 1 Buchstabe c oder d ausgestellt wurde; oder

b. bei der Übertragung der sicherheitsempfindlichen Tätigkeit von den empfohlenen Auflagen der Fachstelle PSP abweicht.

Art. 48 Verwendung einer Erklärung für andere Tätigkeiten

Auf die Durchführung einer Personensicherheitsprüfung kann verzichtet werden, wenn für die zu prüfende Person bereits eine mindestens gleichwertige Erklärung ausgestellt wurde für:

a. eine andere sicherheitsempfindliche Tätigkeit nach dem vorliegenden Gesetz;

b. eine Tätigkeit nach anderen Bundesgesetzen, für deren Ausübung eine Prüfung der Vertrauenswürdigkeit erforderlich ist.

Art. 49 Personensicherheitsbescheinigung im internationalen Verhältnis

Die zuständige Fachstelle PSP stellt auf Antrag hin eine Personensicherheitsbescheinigung im internationalen Verhältnis aus, sofern sie für die betroffene Person eine entsprechende Sicherheitserklärung ausgestellt hat.

Art. 50 Wiederholung

[1] Die Personensicherheitsprüfung wird wie folgt wiederholt:

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

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

[2] Hat die einleitende oder die übertragende Stelle Grund anzunehmen, dass seit der letzten Prüfung neue Risiken entstanden sind, so kann sie bei der zuständigen Fach-

stelle PSP jederzeit mit schriftlicher Begründung eine Wiederholung der Personensicherheitsprüfung verlangen.

Art. 51 Rechtsschutz

[1] Die geprüfte Person hat nach Erhalt der Erklärung nach Artikel 43 Absatz 1 zehn Tage Zeit, um:

a. Einsicht in die Prüfungsunterlagen zu nehmen;

b. die Berichtigung falscher Daten zu verlangen;

c. bei Akten der Fachstellen die Entfernung nicht mehr aktueller Daten zu verlangen;

d. einen Bestreitungsvermerk anbringen zu lassen.

[2] Für die Einschränkung der Auskunft gilt Artikel 9 des Bundesgesetzes vom 19. Juni 1992[7] über den Datenschutz (DSG).

[3] Die Fachstellen PSP erlassen über das Ergebnis ihrer Prüfung eine Verfügung, wenn die geprüfte Person dies innert 30 Tagen nach Erhalt der Erklärung verlangt.

5. Abschnitt: Bearbeitung von Personendaten

Art. 52 Informationssystem zur Personensicherheitsprüfung

[1] Die Fachstelle PSP setzten ein Informationssystem zur Durchführung und Bewirtschaftung der Personensicherheitsprüfungen ein.

[2] Jede Fachstelle PSP ist für die rechtmässige, zweckmässige und verhältnismässige Bearbeitung der Personendaten verantwortlich, die sie im Informationssystem bearbeitet.

[3] Im Informationssystem können besonders schützenswerte Personendaten und Persönlichkeitsprofile nach Artikel 3 Buchstaben c und d DSG[8] bearbeitet werden, sofern dies zur Beurteilung des Sicherheitsrisikos erforderlich ist.

[4] Das Informationssystem enthält folgende Daten:

a. Daten zur Identität der zu prüfenden oder der geprüften Personen;

b. die für die Personensicherheitsprüfung erhobenen Daten nach Artikel 39;

c. die Beurteilung des Sicherheitsrisikos;

d. das Ergebnis der Beurteilung nach Artikel 43 Absatz 1 mit Identität, Adresse, AHV-Versichertennummer, Prüfstufe, Datum und Ablaufdatum;

e. den Entscheid der übertragenden Stelle;

7 SR **235.1**
8 SR **235.1**

f. Daten und Akten aus allfälligen 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.

Art. 53 Datenbekanntgabe

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

a. die Fachstellen PSP: alle Daten nach Artikel 52 Absatz 4;

b. die einleitenden Stellen nach Artikel 36: Daten nach Artikel 52 Absatz 4 Buchstabe b, die sie anlässlich der Einleitung der Prüfung selber erfasst haben, sowie Daten nach Artikel 52 Absatz 4 Buchstaben a, d und e;

c. die übertragenden Stellen nach Artikel 44 Absatz 1: Daten nach Artikel 52 Absatz 4 Buchstaben a, d und e;

d. die Informationssicherheitsbeauftragten nach Artikel 84 zur Erfüllung ihrer Kontrollaufgaben: Daten nach Artikel 52 Absatz 4 Buchstaben a, d und e;

e. die Dienststellen des Bundes und der Kantone, bei denen Daten nach Artikel 39 erhoben werden, als Auftrag zur Lieferung der entsprechenden Daten: Daten nach Artikel 52 Absatz 4 Buchstabe a.

[2] Die folgenden Stellen haben zu den nachstehenden Zwecken über eine Schnittstelle Zugriff auf die Daten nach Artikel 52 Absatz 4 Buchstabe d:

a. die Fachstelle BS nach Artikel 59 zur Durchführung des Betriebssicherheitsverfahrens über eine Schnittstelle zum Informationssystem nach Artikel 77.

b. der Armeestab zur Bearbeitung von Anträgen für Besuche ins Ausland mit Zugang zu klassifizierten Informationen über eine Schnittstelle zum Informationssystem nach den Artikeln 156-161 des Bundesgesetzes vom 3. Oktober 2008[9] über die militärischen Informationssysteme (MIG);

c. der Führungsstab der Armee:

1. zur Kontrolle des Zutritts zu Sicherheitszonen nach Artikel 31 oder zu Anlagen nach der Gesetzgebung über den Schutz militärischer Anlagen über eine Schnittstelle zum Informationssystem nach den Artikeln 162-167 MIG;

2. zur Erfüllung seiner gesetzlichen Aufgaben nach Artikel 13 MIG über eine Schnittstelle zum Informationssystem nach den Artikeln 12-17 MIG;

3. zur Durchführung der Rekrutierung der Stellungspflichtigen sowie des für die Friedensförderung vorgesehenen Personals über eine Schnittstelle zum Informationssystem nach den Artikeln 18-23 MIG.

9 SR **510.91**

[3] Die zuständige Fachstelle PSP kann zudem Daten nach Artikel 52 Absatz 4 Buchstabe d weiterer Organisationen des Bundes elektronisch bekannt geben, wenn diese Daten zur Kontrolle des Zutritts zu Sicherheitszonen nach Artikel 31 erforderlich sind.

[4] Die Fachstellen PSP können den verpflichteten Behörden und Organisationen Listen und Statistiken nach Absatz 1 Buchstabe g bekanntgeben, sofern diese die Daten für die Erfüllung ihrer Kontrollaufgaben nach diesem Gesetz benötigen. Die Listen und Statistiken dürfen nur Personendaten aus dem Zuständigkeitsbereich der betroffenen Behörde oder Organisation enthalten.

Art. 54 Datenaufbewahrung und -vernichtung

[1] Die Fachstellen PSP können die Befragungen nach Artikel 39 Absatz 2 Buchstabe d sowie Absatz 5 mittels technischer Geräte aufnehmen und auf entsprechenden Datenträgern aufbewahren.

[2] Sie bewahren die Daten so lange auf, wie die betreffende Person die Funktion ausübt oder den Auftrag bearbeitet, längstens jedoch zehn Jahre.

[3] Tritt eine geprüfte Person die vorgesehene Funktion nicht an oder lehnt sie die Bearbeitung des vorgesehenen Auftrags ab, so werden alle Daten und Akten vernichtet.

[4] Die Fachstellen PSP vernichten zudem umgehend Daten:

a. die dem Zweck der Bearbeitung nicht entsprechen;

b. deren Bearbeitung aus anderen Gründen unzulässig ist; oder

c. die unrichtig sind.

[5] Bei Daten, die ausserhalb des Informationssystems aufbewahrt werden, vernichten die Fachstellen PSP gleichzeitig die entsprechenden Bearbeitungsvermerke nach Artikel 52 Absatz 5.

[6] Vorbehalten bleibt die Archivierung der Daten nach den Vorschriften der Archivierungsgesetzgebung.

6. Abschnitt: Ergänzende Bestimmungen des Bundesrats

Art. 55

Der Bundesrat erlässt ergänzende Bestimmungen über:

a. das Verfahren der Personensicherheitsprüfung;

b. die Organisation der Fachstellen PSP;

c. die Verantwortung für den Datenschutz in Zusammenhang mit dem Informationssystem nach Artikel 52;

c. die Datensicherheit;

d. die periodische unabhängige Kontrolle der rechtmässigen Bearbeitung von Personendaten.

4. Kapitel: Betriebssicherheitsverfahren

1. Abschnitt: Allgemeine Bestimmungen

Art. 56 Verfahrenszweck

Das Betriebssicherheitsverfahren dient zur Wahrung der Informationssicherheit bei der Vergabe von öffentlichen Aufträgen an Unternehmen oder Teile von Unternehmen (Betriebe), sofern diese Aufträge die Ausübung einer sicherheitsempfindlichen Tätigkeit einschliessen (sicherheitsempfindliche Aufträge).

Art. 57 Betroffene Betriebe

[1] Ein Betriebssicherheitsverfahren wird durchgeführt bei Betrieben:

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

b. mit Sitz in der Schweiz, die sich um Aufträge ausländischer oder internationaler Behörden bewerben, für deren Ausführung eine Betriebssicherheitsbescheinigung nach Artikel 73 erforderlich ist.

[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. 58 Einstellung des Verfahrens

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

a. seine Einwilligung zurückzieht oder am Verfahren nicht mitwirkt;

b. seine Offerte zurückzieht;

c. den Zuschlag nicht erhält; oder

d. aus einem anderen Grund nicht mehr für den Auftrag in Frage kommt.

[2] Wird das Verfahren eingestellt, so werden alle damit zusammenhängenden Daten und Akten vernichtet.

2. Abschnitt: Einleitung des Verfahrens; Sicherheitsanforderungen

Art. 59 Antrag zur Einleitung

[1] Verpflichtete Behörden und Organisationen beantragen der für die Durchführung des Betriebssicherheitsverfahrens zuständigen Fachstelle für Betriebssicherheit (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 ausländische oder internationale Aufträge wird der Antrag durch die zuständige ausländische oder internationale Behörde gestellt.

Art. 60 Prüfung des Antrags

[1] Sind die Voraussetzungen für die Durchführung eines Betriebssicherheitsverfahrens erfüllt, so leitet die Fachstelle BS das Verfahren ein.

[2] Die Fachstelle BS kann auf die Einleitung des Verfahrens verzichten, wenn das Sicherheitsrisiko mit anderen Massnahmen hinreichend reduziert werden kann. Sie empfiehlt entsprechende Massnahmen.

Art. 61 Festlegung der Sicherheitsanforderungen

Nach der Einleitung des Verfahrens legt die Fachstelle BS in Absprache mit der den Auftrag vergebenden Behörde oder Organisation (Auftraggeberin) die Anforderungen an die Informationssicherheit für das Vergabeverfahren sowie für die Auftragserfüllung fest.

3. Abschnitt: Eignung der Betriebe in Bezug auf die Informationssicherheit

Art. 62 Beurteilung der Eignung

[1] Die Auftraggeberin meldet der Fachstelle BS, 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] Die Fachstelle BS ist für die Beurteilung der Eignung der Betriebe weisungsungebunden.

Art. 63 Datenerhebung

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

a. beim Betrieb;

b. beim Nachrichtendienst des Bundes;

c. aus öffentlich zugänglichen Quellen.

[2] Sie kann ausländische Dienststellen um die Zustellung von Daten ersuchen, die den Daten nach Absatz 1 entsprechen.

Art. 64 Sicherheitsrisiko

[1] Ein Sicherheitsrisiko besteht, wenn aufgrund der erhobenen Daten konkrete Anhaltspunkte vorliegen, dass der Betrieb mit hoher Wahrscheinlichkeit den sicherheitsempfindlichen Auftrag 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 ausländischen 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 vereinbart werden kann;

c. für Personen des Betriebs, die für die Ausführung des sicherheitsempfindlichen Auftrags unentbehrlich sind, eine Risikoerklärung nach Artikel 43 Absatz 1 Buchstabe c ausgestellt wird.

[3] Das Sicherheitsrisiko muss ungeachtet eines Verschuldens durch die tatsächlichen Umstände und Verhältnisse des betroffenen Betriebs begründet werden.

Art. 65 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 ein Sicherheitsrisiko darstellt, so schliesst die Auftraggeberin den betreffenden Betrieb vom Vergabeverfahren aus.

4. Abschnitt: Sicherheitskonzept; Betriebssicherheitserklärung

Art. 66 Sicherheitskonzept

[1] Die Auftraggeberin meldet der Fachstelle BS, welcher Betrieb den Zuschlag erhalten hat.

[2] Die Fachstelle BS erstellt für den Betrieb ein Sicherheitskonzept.

[3] Sie kann die dazu nötigen Daten schriftlich oder mittels einer Betriebsbesichtigung erheben.

Art. 67 Personensicherheitsprüfungen

[1] Personen des Betriebs, die eine sicherheitsempfindliche Tätigkeit ausüben sollen, werden einer Personensicherheitsprüfung unterzogen.

[2] Die Fachstelle BS ist für den Entscheid nach Artikel 46 Absatz 2 zuständig.

Art. 68 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 Gültigkeit der Betriebssicherheitserklärung beträgt fünf Jahre.

5. Abschnitt: Folgen der Betriebssicherheitserklärung

Art. 69 Ausführung des sicherheitsempfindlichen Auftrags

Die Auftraggeberin ist an die Verfügung der Fachstelle BS gebunden. Sie darf den sicherheitsempfindlichen Auftrag erst ausführen lassen, nachdem die Betriebssicherheitserklärung ausgestellt wurde.

Art. 70 Pflichten des Betriebs

[1] Betriebe mit einer Betriebssicherheiterklärung müssen die Massnahmen des Sicherheitskonzepts laufend umsetzen.

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

Art. 71 Kontrollen und Schutzmassnahmen

[1] Die Fachstelle BS ist befugt:

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

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 Materialien sicherstellen.

Art. 72 Vereinfachtes Verfahren bei der Vergabe weiterer sicherheitsempfindlicher Aufträge

[1] Bei der Vergabe weiterer sicherheitsempfindlicher Aufträge gelten Betriebe, die über eine Betriebssicherheitserklärung verfügen, im Sinne von Artikel 62 als geeignet.

[2] Erhält ein solcher Betrieb den Zuschlag, so prüft die Fachstelle BS, ob das bestehende Sicherheitskonzept angepasst werden muss.

Art. 73 Betriebssicherheitsbescheinigung im internationalen Verhältnis

Die Fachstelle BS stellt dem Betrieb auf dessen Antrag hin eine Betriebssicherheitsbescheinigung im internationalen Verhältnis aus.

6. Abschnitt: Widerruf der Betriebssicherheitserklärung, Wiederholung des Verfahrens und Rechtsschutz

Art. 74 Widerruf der Betriebssicherheitserklärung

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

a. der Betrieb seine Pflichten nach Artikel 70 nicht erfüllt;

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

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

Art. 75 Wiederholung des Verfahrens

Das Betriebssicherheitsverfahren wird wiederholt, wenn:

a. beim Ablauf der Betriebssicherheitserklärung noch ein sicherheitsempfindlicher Auftrag hängig ist;

b. konkreter Grund zur Annahme besteht, dass in Folge wesentlicher Änderungen im Betrieb neue Sicherheitsrisiken entstanden sind.

Art. 76 Rechtsschutz

[1] Die Organe des Betriebs haben nach Eröffnung der Verfügungen der Fachstelle BS zehn Tage Zeit, um:

a. Einsicht in die Unterlagen zu nehmen;

b. die Berichtigung falscher Daten zu verlangen;

c. bei Akten der Fachstelle BS die Entfernung nicht mehr aktueller Daten zu verlangen;

d. einen Bestreitungsvermerk anbringen zu lassen.

[2] Für die Einschränkung der Auskunft gilt Artikel 9 des Bundesgesetzes vom 19. Juni 1992[10] über den Datenschutz (DSG).

10 SR **235.1**

[3] Gegen die Verfügungen der Fachstelle BS kann beim Bundesverwaltungsgericht Beschwerde geführt werden.

7. Abschnitt: Bearbeitung von Personendaten

Art. 77 Informationssystem zum Betriebssicherheitsverfahren

[1] Die Fachstelle BS setzt zur Durchführung des Betriebssicherheitsverfahrens und der damit zusammenhängenden Personensicherheitsprüfungen ein Informationssystem ein.

[2] Im Informationssystem können besonders schützenswerte Personendaten und Persönlichkeitsprofile nach Artikel 3 Buchstaben c und d DSG[11] bearbeitet werden, sofern dies zur Durchführung des Betriebssicherheitsverfahrens erforderlich ist.

[3] Das Informationssystem enthält folgende Daten:

a. die für das Betriebssicherheitsverfahren erhobenen Daten nach den Artikeln 63 und 66 Absatz 3;

b. das Ergebnis der Beurteilung nach Artikel 62 Absatz 2;

c. die Ergebnisse der für das Betriebssicherheitsverfahren erforderlichen Personensicherheitsprüfungen nach Artikel 67 Absatz 1;

d. den Entscheid der Fachstelle BS nach Artikel 67 Absatz 2;

e. die Namen aller Betriebe mit einer Betriebssicherheitserklärung, inklusive Ausstellungsdatum;

f. die Massnahmen allfälliger Kontrollen nach Artikel 71;

g. Daten und Akten aus allfälligen Beschwerdeverfahren.

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

Art. 78 Datenbekanntgabe

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

a. die Auftraggeberinnen nach Artikel 61: Daten nach Artikel 77 Absatz 3 Buchstaben b und d-g;

b. die betroffenen Betriebe, sofern sie vom Bundesrat gestützt auf Artikel 36 ermächtigt worden sind, Personensicherheitsprüfungen in ihrem Zuständigkeitsbereich einzuleiten: Daten nach Artikel 77 Absatz 3 Buchstaben c und d.

11 SR **235.1**

Art. 79 Datenaufbewahrung und -vernichtung

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

[2] Sie vernichtet umgehend Daten:

a. die dem Zweck der Bearbeitung nicht entsprechen;

b. deren Bearbeitung aus anderen Gründen unzulässig ist; oder

c. die unrichtig sind.

[3] Vorbehalten bleibt die Archivierung der Daten nach den Vorschriften der Archivierungsgesetzgebung.

8. Abschnitt: Ergänzende Bestimmungen des Bundesrats

Art. 80

Der Bundesrat erlässt ergänzende Bestimmungen über:

a. das Verfahren des Betriebssicherheitsverfahrens;

b. die Datenbearbeitung, das Informationssystem und die Datensicherheit;

c. die Organisation der Fachstelle BS.

5. Kapitel: Informationssicherheit bei kritischen Infrastrukturen

Art. 81 Aufgaben des Bundes

[1] Der Bund unterstützt die Betreiberinnen und Betreiber von kritischen Infrastrukturen im Bereich der Informationssicherheit insbesondere bei:

a. der frühzeitigen Identifizierung und Bewertung der Bedrohungen und Gefahren;

b. der Erkennung von Vorfällen;

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

d. der Nachbearbeitung von Vorfällen.

[2] Er führt einen nationalen Frühwarnungsdienst und eine Anlaufstelle für präventive und reaktive Massnahmen im Bereich der technischen Informationssicherheit.

[3] Er sorgt dafür, dass die Betreiberinnen und Betreiber von kritischen Infrastrukturen mit den zuständigen Stellen des Bundes und untereinander Informationen über Bedrohungen, Risiken und Vorfälle sicher austauschen können.

Art. 82 Bearbeitung von Personendaten

[1] Die zuständigen Stellen nach Artikel 81 dürfen zur Abwehr von Gefahren Personendaten, insbesondere Adressierungselemente im Fernmeldebereich, bearbeiten und den verpflichteten Behörden und Organisationen, den zuständigen Stellen der Kantone sowie Dritten bekanntgeben, sofern dies zu deren Aufgabenerfüllung notwendig ist. Die Bearbeitung kann erfolgen, ohne dass dies für die betroffenen Personen ersichtlich ist.

[2] Absatz 1 gilt auch für besonders schützenswerte Personendaten, die im Zusammenhang mit administrativen oder strafrechtlichen Verfolgungen und Sanktionen stehen.

[3] Die Betreiberinnen und Betreiber von IKT-Mitteln sowie die Anbieterinnen und Anbieter von IKT-Diensten dürfen vorfallbezogene Personendaten nach Absatz 1 den zuständigen Stellen nach Artikel 81 bekanntgeben, ohne dass dies für die betroffenen Personen ersichtlich ist. Diese Daten dürfen nicht für gerichtliche Verfahren verwendet werden.

Art. 83 Ergänzende Bestimmungen des Bundesrats

Der Bundesrat erlässt ergänzende Bestimmungen über:

a. die Aufgabenteilung und die Zusammenarbeit zwischen den Stellen, welche die Aufgaben nach Artikel 81 wahrnehmen, und dem Nachrichtendienst des Bundes;

b. den Austausch nachrichtendienstlicher Informationen durch die in Buchstabe a aufgeführten Stellen und deren Bekanntgabe an Betreiberinnen und Betreiber Kritischer Infrastrukturen;

c. die Datenbearbeitung durch die Stellen, welche die Aufgaben nach Artikel 81 wahrnehmen, sowie die Datensicherheit.

6. Kapitel: Organisation und Vollzug

1. Abschnitt: Organisation

Art. 84 Informationssicherheitsbeauftragte

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

a. der Bundesrat;

b. die Verwaltungsdelegation der Bundesversammlung;

c. die eidgenössischen Gerichte;

d. die Bundesanwaltschaft;

e. die Schweizerische Nationalbank;

f. die Departemente und die Bundeskanzlei.

[2] Die Informationssicherheitsbeauftragten haben folgende Aufgaben:

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

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

c. Sie überprüfen regelmässig die Einhaltung der Vorgaben der Informationssicherheit, erstatten Bericht und beantragen ihrer Behörde die erforderlichen Massnahmen.

d. Sie können der Fachstelle des Bundes für Informationssicherheit, der Konferenz der Informationssicherheitsbeauftragten sowie den Stellen, welche die Aufgaben nach Artikel 81 wahrnehmen, sicherheitsrelevante Vorfälle melden.

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

Art. 85 Konferenz der Informationssicherheitsbeauftragten

[1] Die Konferenz der Informationssicherheitsbeauftragten wird aus den Informationssicherheitsbeauftragten nach Artikel 84 Absatz 1 gebildet.

[2] Sie hat folgende Aufgaben:

a. Sie fördert den einheitlichen, behördenübergreifenden Vollzug dieses Gesetzes.

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

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

d. Sie sorgt für die Koordination mit der oder dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten sowie mit den anderen Stellen, die Aufgaben im Bereich der Informationssicherheit wahrnehmen.

[3] Die Konferenz erlässt ihr Geschäftsreglement.

Art. 86 Fachstelle des Bundes für Informationssicherheit

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

a. Sie berät und unterstützt die verpflichteten Behörden und deren Informationssicherheitsbeauftragte beim Vollzug dieses Gesetzes, insbesondere bei der Steuerung der Informationssicherheit sowie beim Risikomanagement.

b. Sie empfiehlt bei Gefährdung der Informationssicherheit des Bundes Sofortmassnahmen.

c. Sie führt im Auftrag der verpflichteten Behörden Kontrollen und Überprüfungen durch.

d. Sie beurteilt im Auftrag der verpflichteten Behörden die Risiken für die Informationssicherheit beim Einsatz neuartiger Technologien.

e. Sie prüft auf Antrag der verpflichteten Behörden und Organisationen die Eignung bestimmter Prozesse, Mittel, Einrichtungen, Gegenstände und Dienstleistungen auf sicherheitsrelevante Aspekte.

f. Sie steuert und koordiniert auf Antrag der verpflichteten Behörden die Belange der Informationssicherheit bei wichtigen behördenübergreifenden Projekten.

g. Sie ist Ansprechstelle für Fachkontakte mit inländischen, ausländischen und internationalen Stellen im Bereich der Informationssicherheit.

h. Sie erstattet dem Bundesrat jährlich Bericht über den Stand der Informationssicherheit im Bund.

[2] Die oder der Informationssicherheitsbeauftragte des Bundesrates 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.

2. Abschnitt: Vollzug

Art. 87 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, welche 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 für ihren Zuständigkeitsbereich keine eigenen Ausführungsbestimmungen nach Absatz 1 erlassen.

[4] Der Bundesrat legt durch Verordnung fest, welche Organisationen nach Artikel 2 Absatz 2 Buchstabe e das Gesetz ganz oder teilweise anwenden müssen.

Art. 88 Standardanforderungen und -massnahmen

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

[2] Er kann diese Aufgabe an die Fachstelle des Bundes für Informationssicherheit oder an andere fachkompetente Stellen delegieren.

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

Art. 89 Kantone

[1] Die Kantone sorgen dafür, dass kantonale Behörden und Stellen, die im Auftrag des Bundes und unter seiner Aufsicht sicherheitsempfindliche Tätigkeiten ausüben, die Massnahmen nach diesem Gesetz umsetzen.

[2] Der Bundesrat regelt:

a. die Personensicherheitsprüfungen für kantonale Organe;

b. die Kontrolle der Massnahmen nach Absatz 1.

[3] Die Kantone bezeichnen für Fragen der Informationssicherheit je eine Dienststelle als Ansprechpartner für die Bundesbehörden.

Art. 90 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 bei kritischen Infrastrukturen;

b. zum Austausch von klassifizierten Informationen;

c. zur gegenseitigen Durchführung von Personensicherheitsprüfungen und Betriebssicherheitsverfahren;

d. zur gegenseitigen Anerkennung von Sicherheitserklärungen;

e. zur Durchführung von gegenseitigen Kontrollen.

Art. 91 Evaluation

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

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

7. Kapitel: Schlussbestimmungen

Art. 92 Änderung anderer Erlasse

Die Änderung anderer Erlasse wird im Anhang geregelt.

Art. 93 Übergangsbestimmungen

[1] Personensicherheitserklärungen und Betriebssicherheitserklärungen nach bisherigem Recht bleiben bis zu ihrem Ablauf gültig.

[2] Der Bundesrat bestimmt die Übergangsfristen für die Anpassung an:

a. die Vorschriften über die Klassifizierung;

b. die Vorschriften über die Sicherheit beim Einsatz von IKT-Mitteln.

Art. 94 Referendum und Inkrafttreten

[1] Dieses Gesetz untersteht dem fakultativen Referendum.

[2] Der Bundesrat bestimmt das Inkrafttreten.

Anhang
(Art. 92)

Änderung anderer Erlasse

1. Bundesgesetz vom 21. März 1997[12] über Massnahmen zur Wahrung der inneren Sicherheit

Art. 2 Abs. 4 Bst. c

Aufgehoben

Art. 19-21

Aufgehoben

2. Archivierungsgesetz vom 26. Juni 1998[13]

Art. 6 Abs. 2

[2] Klassifizierte Unterlagen müssen vor der Abgabe an das Bundesarchiv nach den Bestimmungen der Gesetzgebung über die Informationssicherheit entklassifiziert werden.

3. Bundespersonalgesetz vom 24. März 2000[14]

Art. 20a Auszug aus dem Strafregister und dem Betreibungsregister

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

Art. 20b Prüfung der Vertrauenswürdigkeit

[1] Der Bundesrat kann Stellenbewerberinnen und Stellenbewerber sowie Angestellte auf ihre Vertrauenswürdigkeit hin prüfen lassen, wenn sie im Rahmen ihrer Funktion:

12 SR **120**
13 SR **152. 1**
14 SR **172.220.1**

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

b. Entscheidungskompetenzen oder Aufsichtsaufgaben in wesentlichen Finanz- oder Steuersachen erfüllen 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 Mindestmass, das für die Wahrung der Interessen des Bundes erforderlich ist.

[3] Das Prüfverfahren richtet sich sinngemäss nach den Bestimmungen über die Personensicherheitsprüfung des Bundesgesetzes vom ... [15] über die Informationssicherheit.

[4] Werden die Stellenbewerberinnen und Stellenbewerber sowie die Angestellten nach Absatz 1 gleichzeitig einer Personensicherheitsprüfung nach dem Bundesgesetz über die Informationssicherheit unterzogen, so werden die beiden Verfahren vereinigt.

4. Strafgesetzbuch vom 21. Dezember 1937[16]

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 Bundesgesetz vom ... [17] über die Informationssicherheit und der Prüfungen der Vertrauenswürdigkeit nach der Spezialgesetzgebung;

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

[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 Fachstellen für Personensicherheitsprüfungen nach dem Bundesgesetz über die Informationssicherheit;

[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 für Personensicherheitsprüfungen nach dem Bundesgesetz über die Informationssicherheit;

15 SR ...
16 SR **311.0**
17 SR ...

5. Bundesgesetz vom 13. Juni 2008[18] über die polizeilichen Informationssysteme des Bundes

Art. 15 Abs. 4 Bst. f

[4] Folgende Behörden dürfen zur Erfüllung ihrer Aufgaben mittels Abrufverfahren Daten aus dem Informationssystem abrufen:

f. die Fachstellen für Personensicherheitsprüfungen nach dem Bundesgesetz vom ... [19] über die Informationssicherheit zur Beurteilung des Sicherheitsrisikos im Rahmen einer Personensicherheitsprüfung, einer Prüfung der Vertrauenswürdigkeit oder einer Beurteilung des Gewaltpotenzials;

Art. 17 Abs. 4 Bst. l

[4] Zugriff auf diese Daten mittels eines automatisierten Abrufverfahrens haben:

l. die Fachstellen für Personensicherheitsprüfungen nach dem Bundesgesetz vom ... [20] über die Informationssicherheit zur Beurteilung des Sicherheitsrisikos im Rahmen einer Personensicherheitsprüfung, einer Prüfung der Vertrauenswürdigkeit oder einer Beurteilung des Gewaltpotenzials;

6. Militärgesetz vom 3. Februar 1995[21]

Art. 14 Prüfung der Vertrauenswürdigkeit

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

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

b. Entscheidungskompetenzen oder Aufsichtsaufgaben in wesentlichen finanziellen Angelegenheiten erfüllen 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 Mindestmass, das für die Wahrung der Interessen des Bundes erforderlich ist.

[3] Das Prüfverfahren richtet sich sinngemäss nach den Bestimmungen über die Personensicherheitsprüfung des Bundesgesetzes vom ... [22] über die Informationssicherheit.

18 SR **361**
19 SR ...
20 SR ...
21 SR **510.10**
22 SR ...

[4] Werden die Angehörigen der Armee nach Absatz 1 gleichzeitig einer Personensicherheitsprüfung nach dem Bundesgesetz über die Informationssicherheit unterzogen, so werden die beiden Verfahren vereinigt.

Art. 113 Abs. 5

[5] Das Verfahren richtet sich sinngemäss nach den Bestimmungen über die Grundsicherheitsprüfung nach Artikel 35 Buchstabe a des Bundesgesetzes vom ...[23] über die Informationssicherheit. Ist gleichzeitig aus anderen Gründen eine Grundsicherheitsprüfung durchzuführen, so werden die beiden Verfahren vereinigt.

Art. 150 Abs. 4

Aufgehoben

7. Bundesgesetz vom 3. Oktober 2008[24] über die militärischen Informationssysteme

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

Aufgehoben

8. Kernenergiegesetz vom 21. März 2003[25]

Art. 5

[3] Um zu verhindern, dass die nukleare Sicherheit von Kernanlagen und Kernmaterialien durch unbefugtes Einwirken beeinträchtigt oder Kernmaterialien entwendet werden, müssen Sicherungsmassnahmen getroffen werden. Diese Massnahmen sind, soweit erforderlich, nach den Bestimmungen des Bundesgesetzes vom ...[26] über die Informationssicherheit zu klassifizieren und zu bearbeiten.

Art. 24 Prüfung der Vertrauenswürdigkeit

[1] Personen, die Aufgaben erfüllen sollen, die für die nukleare Sicherheit oder die Sicherung der Kernanlage wesentlich sind, werden zur Beurteilung des Sicherheitsrisikos auf ihre Vertrauenswürdigkeit hin geprüft.

[2] Der Bundesrat legt fest, welche Personengruppen geprüft werden müssen.

23 SR **...**
24 SR **510.91**
25 SR **732.1**
26 SR ...

[3] Das Prüfverfahren richtet sich sinngemäss nach den Bestimmungen über die Personensicherheitsprüfung des Bundesgesetzes vom ...[27] über die Informationssicherheit.

[4] Die Daten aus der Prüfung dürfen dem Eigentümer der Kernanlage und der Aufsichtsbehörde bekannt gegeben werden.

9. Stromversorgungsgesetz vom 23. März 2007[28]

Gliederungstitel vor Art. 25

6. Kapitel: Auskunftspflicht, Amts- und Geschäftsgeheimnis, Prüfung der Vertrauenswürdigkeit, Aufsichtsabgabe

Art. 26a 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.

[3] Das Prüfverfahren richtet sich sinngemäss nach den Bestimmungen über die Personensicherheitsprüfung des Bundesgesetzes vom ...[29] über die Informationssicherheit.

[4] Die Daten aus der Prüfung dürfen der Geschäftsleitung der nationalen Netzgesellschaft, dem Bundesamt und der ElCom bekannt gegeben werden.

10. Nationalbankgesetz vom 3. Oktober 2003[30]

Art. 16 Sachüberschrift und Abs. 5

Vertraulichkeit und Informationssicherheit

[5] Die Nationalbank wendet für ihren Bereich das Bundesgesetz vom ... [31] über die Informationssicherheit an. Im Übrigen gelten die Bestimmungen des Bundesgesetzes vom 19. Juni 1992[1] über den Datenschutz.

27 SR **...**
28 SR **734.7**
29 SR ...
30 SR **951.11**

31 SR ...