Bundesgesetz über die Informationssicherheit (Informationssicherheitsgesetz, ISG)[1]

vom 18. Dezember 2020 (Stand am 1. April 2025)

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[2],
nach Einsicht in die Botschaft des Bundesrates vom 22. Februar 2017[3],
beschliesst:

1. Kapitel: Allgemeine Bestimmungen

Art. 1 Zweck

[1] Dieses Gesetz soll:

a. die sichere Bearbeitung der Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz der Informatikmittel des Bundes gewährleisten;

b. die Widerstandsfähigkeit der Schweiz gegenüber Cyberbedrohungen erhöhen.[4]

[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.

AS **2022** 232

1 Fassung gemäss Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).
2 SR **101**
3 BBl **2017** 2953
4 Fassung gemäss Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

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;

d. die Bundesanwaltschaft und die Aufsichtsbehörde über die 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[5] (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 73*a*–79.[6] Die Spezialgesetzgebung kann weitere Teile dieses Gesetzes für anwendbar erklären.

Art. 3 Geltung für die Kantone

[1] Für die Kantone gelten nur die Bestimmungen:

a. über klassifizierte Informationen, soweit sie klassifizierte Informationen des Bundes bearbeiten; und

b. über die Sicherheit beim Einsatz von Informatikmitteln, soweit sie auf Informatikmittel des Bundes zugreifen.

5 SR **172.010**

6 Fassung gemäss Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

2 Diese 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[7] (BGÖ) geht diesem Gesetz vor.[8]

1bis Informationen Dritter, von denen das Bundesamt für Cybersicherheit (BACS) durch die Entgegennahme und Analyse von Meldungen gemäss dem 5. Kapitel Kenntnis erhält, dürfen nicht nach dem BGÖ zugänglich gemacht werden. Nicht als Dritte gelten Behörden, Organisationen und Personen nach Artikel 2 Absatz 1 BGÖ.[9]

2 Für Informationen, deren Schutz auch 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:* Trinkwasser- und Energieversorgung, Informations-, Kommunikations- und Transportinfrastrukturen sowie weitere Prozesse, Systeme und Einrichtungen, die essenziell für das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung sind;

7 SR **152.3**
8 Fassung gemäss Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).
9 Eingefügt durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 168, 173; BBl **2023** 84).

d.[10] *Cybervorfall:* Ereignis bei der Nutzung von Informatikmitteln, das dazu führt, dass die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist;

e.[11] *Cyberangriff:* Cybervorfall, der absichtlich ausgelöst wurde;

f.[12] *Cyberbedrohung:* Jeder Umstand oder jedes Ereignis mit dem Potenzial, einen Cybervorfall zu ermöglichen;

g.[13] *Schwachstelle:* Cyberbedrohung, die auf Schwächen oder Fehler in Informatikmitteln zurückzuführen ist.

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).

[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.

10 Eingefügt durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

11 Eingefügt durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

12 Eingefügt durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

13 Eingefügt durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

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.

Art. 10*a*[14] Bearbeitung von Personendaten

[1] Die verpflichteten Behörden und Organisationen können die zur Gewährleistung der Informationssicherheit zweckmässigen Personendaten, insbesondere in dafür vorgesehenen Informationssystemen (ISMS-Anwendungen), bearbeiten.

14 Eingefügt durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

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

a. dies zur Gewährleistung der Informationssicherheit zweckmässig ist;

b. keine gesetzlichen oder vertraglichen Geheimhaltungspflichten verletzt werden;

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

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

3 Sie können ihre Informationssysteme, insbesondere die ISMS-Anwendungen, miteinander verknüpfen und Daten automatisch oder auf Anfrage über Schnittstellen austauschen.

4 Sie können zur Einreichung und Bearbeitung von Anträgen und Meldungen im Bereich der Informationssicherheit digitale Formulare betreiben und diese mit ihren ISMS-Anwendungen oder anderen Informationssystemen verknüpfen.

5 Sofern dies für die Bewältigung von Verletzungen der Informationssicherheit oder die Behebung von Schwachstellen erforderlich ist, können sie besonders schützenswerte Personendaten nach Artikel 5 Buchstabe c des Datenschutzgesetzes vom 25. September 2020[15] (DSG) von Personen, die daran beteiligt oder davon betroffen sind respektive sein könnten:

a. bearbeiten;

b. untereinander sowie mit nationalen, internationalen und ausländischen Organisationen des öffentlichen Rechts austauschen, sofern die Bedingung nach Absatz 2 Buchstabe b erfüllt ist.

6 Sie dürfen die besonders schützenswerten Personendaten bis zwei Jahre nach der Bewältigung der Verletzungen der Informationssicherheit oder der Behebung der Schwachstellen aufbewahren, höchstens aber zehn Jahre.

7 Die Archivierung der Daten richtet sich nach den Vorschriften der Archivierungsgesetzgebung.

8 Die Bearbeitung von Personendaten durch das BACS[16] zur Erfüllung seiner Aufgaben richtet sich nach den Artikeln 75–79.

15 SR **235.1**

16 Ausdruck gemäss Ziff. I der V vom 7. März 2025, in Kraft seit 1. April 2025 (AS **2025** 168). Diese Änd. wurde im ganzen Erlass berücksichtigt.

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.

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 87 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 57*i*–57*q* RVOG[17].

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.

3 Sie können zudem die AHV-Nummer nach Artikel 50*c* des Bundesgesetzes vom 20. Dezember 1946[18] über die Alters- und Hinterlassenenversicherung (AHV-Nummer) systematisch als Personenidentifikator verwenden.[19]

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.

17 SR **172.010**
18 SR **831.10**
19 Fassung gemäss Anhang Ziff. 40 des BG vom 18. Dez. 2020 (Systematische Verwendung der AHV-Nummer durch Behörden), in Kraft seit 1. Jan. 2024 (AS **2021** 758; **2023** 650; BBl **2019** 7359).

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[20] (FMG) betreiben.

4 Vorbehalten bleiben die besonderen Vorschriften für Sicherheitszonen gemäss völkerrechtlichen Verträgen nach Artikel 87 sowie für Schutzzonen von Anlagen nach der Gesetzgebung über den Schutz militärischer Anlagen.

20 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 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;
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. 27 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. 28 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. 29 Zu prüfende Personen

1 Eine Personensicherheitsprüfung wird durchgeführt bei:

a. Angestellten des Bundes, externen Mitarbeitenden und Angehörigen der Armee, die eine Funktion ausüben, die in einer Liste nach Artikel 28 enthalten ist;

b. Angestellten eines Kantons, die eine sicherheitsempfindliche Tätigkeit ausüben;

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

d. Personen, die aufgrund eines völkerrechtlichen Vertrags nach Artikel 87 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 87 abgeschlossen hat.

3 Personen, die eine Funktion ausüben, die noch nicht in einer Liste nach Artikel 28 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;

e^bis.[21] Leiterin oder Leiter des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten;

f. General;

g. kantonale Magistratsperson, die vom Volk oder vom kantonalen Parlament gewählt wird.

Art. 30 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. 31 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. 32 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.

21 Eingefügt durch Ziff. I der BG vom 17. Juni 2022 (Leiterin oder Leiter des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten), in Kraft seit 1. Jan. 2024 (AS **2023** 734; BBl **2022** 345, 432).

Art. 33 Zeitpunkt der Personensicherheitsprüfung

[1] Bei Personen nach Artikel 29 Absatz 1 Buchstaben a und b muss die Personensicherheitsprüfung eingeleitet werden, bevor die Funktion übertragen wird.

[2] Bei Personen nach Artikel 29 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 29 Absatz 1 Buchstabe c muss die Personensicherheitsprüfung abgeschlossen sein, bevor sie mit der Ausübung der sicherheitsempfindlichen Tätigkeit beauftragt wird.

[4] Bei Personen nach Artikel 29 Absatz 1 Buchstabe d richtet sich der Zeitpunkt der Personensicherheitsprüfung nach den Bestimmungen des entsprechenden Vertrags.

Art. 34 Datenerhebung

[1] Die 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 die Auskunft freiwillig ist.

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. 35 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 34.

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. 36 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 29 Absatz 1 Buchstabe b.

Art. 37 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. 38 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. 39 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. 40 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[22] 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.

22 SR **510.10**

4. Abschnitt: Folgen der Erklärung

Art. 41 Ausübung der sicherheitsempfindlichen Tätigkeit

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

[2] Die Stelle nach Artikel 31 Absatz 1 Buchstabe b entscheidet nach Kenntnisnahme der 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. 42 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 anderen Bundesgesetz.

Art. 43 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.

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

Art. 44 Rechtsschutz

[1] Die geprüfte Person hat nach Erhalt der Erklärung nach Artikel 39 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 26 DSG[23].[24]

3 Die Erklärung stellt einen Realakt nach Artikel 25*a* des Verwaltungsverfahrensgesetzes vom 20. Dezember 1968[25] dar. Die geprüfte Person kann gegen eine Erklärung nach Artikel 39 Absatz 1 Buchstaben b–d innerhalb von 30 Tagen nach deren Erhalt 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[26] sinngemäss.

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

5. Abschnitt: Bearbeitung von Personendaten

Art. 45 Informationssystem zur Personensicherheitsprüfung

1 Die Fachstellen PSP betreiben ein Informationssystem. Dieses dient der Durchführung von:

a. Personensicherheitsprüfungen;

b. Beurteilungen des Gefährdungs- oder Missbrauchspotenzials bezüglich der persönlichen Waffe;

c. Zuverlässigkeitskontrollen;

d. Prüfungen der Vertrauenswürdigkeit.[27]

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

3 Im Informationssystem können besonders schützenswerte Personendaten nach Artikel 5 Buchstabe c DSG[28] bearbeitet werden, sofern dies zur Beurteilung des Sicherheitsrisikos erforderlich ist.[29]

3bis Anhand der Daten des Informationssystems darf ein Profiling, einschliesslich eines Profilings mit hohem Risiko, nach DSG durchgeführt werden, um die nachfolgenden persönlichen Aspekte einer natürlichen Person zu den Bearbeitungszwecken nach Absatz 1 zu analysieren, zu bewerten, zu beurteilen oder vorherzusagen:

a. Sicherheitsrisiko;

23 SR **235.1**
24 Fassung gemäss Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).
25 SR **172.021**
26 SR **172.220.1**
27 Fassung gemäss Ziff. II 2 des BG vom 17. Juni 2022, in Kraft seit 1. Jan. 2024 (AS **2023** 117, 650; BBl **2021** 3046).
28 SR **235.1**
29 Fassung gemäss Anhang 2 Ziff. 5, in Kraft seit 1. Jan. 2024 (AS **2022** 232; **2023** 650; BBl **2017** 2953).

b. Gefährdungs- und Missbrauchspotenzial bezüglich der persönlichen Waffe.[30]

4 Das Informationssystem enthält folgende Daten:

a.[31] Daten zur Identität der zu prüfenden oder geprüften Personen, einschliesslich der AHV-Nummer und der Passnummer;

b. die Daten nach den Artikeln 34 und 35;

c. die Beurteilung des Sicherheitsrisikos;

d. die Erklärung nach Artikel 39 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.[32] Strafregister-Informationssystem VOSTRA nach dem Strafregistergesetz vom 17. Juni 2016[33];

b. nationaler Polizeiindex nach Artikel 17 des Bundesgesetzes vom 13. Juni 2008[34] über die polizeilichen Informationssysteme des Bundes;

c. INDEX NDB nach Artikel 51 des Nachrichtendienstgesetzes vom 25. September 2015[35];

d.[36] die Datenbanken der Zentralstelle Waffen nach Artikel 32*a* Absatz 1 des Waffengesetzes vom 20. Juni 1997[37].

Art. 46 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 45 Absatz 4 Buchstabe b, die sie anlässlich der Einleitung der Prüfung selber erfasst haben, sowie die Daten nach Artikel 45 Absatz 4 Buchstaben a, d und e;

30 Eingefügt durch Ziff. II 2 des BG vom 17. Juni 2022, in Kraft seit 1. Jan. 2024 (AS **2023** 117, 650; BBl **2021** 3046).
31 Fassung gemäss Anhang Ziff. 40 des BG vom 18. Dez. 2020 (Systematische Verwendung der AHV-Nummer durch Behörden), in Kraft seit 1. Jan. 2024 (AS **2021** 758; **2023** 650; BBl **2019** 7359).
32 Fassung gemäss Anhang 2 Ziff. 4, in Kraft seit 1. Jan. 2024 (AS **2022** 232; **2023** 650; BBl **2017** 2953).
33 SR **330**
34 SR **361**
35 SR **121**
36 Eingefügt durch Ziff. II 2 des BG vom 17. Juni 2022, in Kraft seit 1. Jan. 2024 (AS **2023** 117, 650; BBl **2021** 3046).
37 SR **514.54**

b. entscheidende Stellen: auf die Daten nach Artikel 45 Absatz 4 Buchstaben a, d und e;

c. Informationssicherheitsbeauftragte nach Artikel 81 zur Erfüllung ihrer Kontrollaufgaben: auf die Daten nach Artikel 45 Absatz 4 Buchstaben a, d und e;

d. Stellen des Bundes und der Kantone, bei denen Daten nach Artikel 37 erhoben werden: auf die Daten nach Artikel 45 Absatz 4 Buchstabe a.

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

a. die Fachstelle nach Artikel 51 Absatz 2 zur Durchführung des Betriebssicherheitsverfahrens nach den Artikeln 49–73 über das Informationssystem nach Artikel 70: auf die Daten nach Artikel 45 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[38] über die militärischen Informationssysteme (MIG) über das Personalinformationssystem der Armee nach Artikel 12 MIG: auf die Daten nach Artikel 45 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 45 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 45 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 45 Absatz 4 Buchstaben a und e;

c. die Stelle, die für die Sicherheitsbescheinigung im internationalen Verhältnis nach Artikel 48 Buchstabe c zuständig ist: auf die Daten nach Artikel 45 Absatz 4 Buchstaben a, d und e.

3 Die Fachstellen PSP können zudem Daten nach Artikel 45 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 45 Absatz 1 Buchstabe g bekanntgeben, sofern dies zur Erfüllung von deren Kontrollaufgaben nach diesem Gesetz erforderlich ist.

Art. 47 Datenaufbewahrung, -archivierung und -vernichtung

1 Die Fachstellen PSP können Befragungen nach Artikel 34 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.

38 SR **510.91**

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

[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. 48

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 45 sowie die Datensicherheit;

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

4. Kapitel: Betriebssicherheitsverfahren

1. Abschnitt: Allgemeine Bestimmungen

Art. 49 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. 50 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 66 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. 51 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. 52 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 50 Absatz 1 Buchstabe b stellt die zuständige ausländische Behörde oder internationale Organisation den Antrag.

Art. 53 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. 54 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. 55 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. 56 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. 57 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. 58 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 59, 60, 63 und 64 sinngemäss an.

4. Abschnitt: Sicherheitskonzept

Art. 59 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. 60 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 41 Absatz 2 zuständig. Wird das Verfahren eingestellt, weil sich kein Betrieb für die Ausführung des Auftrags eignet (Art. 58 Abs. 3), so ist die Auftraggeberin für den Entscheid zuständig.

5. Abschnitt: Betriebssicherheitserklärung

Art. 61 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 58 Absatz 3.

5 Die Gültigkeit der Betriebssicherheitserklärung beträgt fünf Jahre.

Art. 62 Ausführung des sicherheitsempfindlichen Auftrags

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

Art. 63 Pflichten des Betriebs

1 Betriebe, die über eine Betriebssicherheitserklärung verfügen, müssen die Massnahmen des Sicherheitskonzepts laufend umsetzen.

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

Art. 64 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. 65 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. 66 Internationale Betriebssicherheitsbescheinigung

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

Art. 67 Widerruf der Betriebssicherheitserklärung

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

a. der Betrieb seine Pflichten nach Artikel 63 nicht erfüllt;

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

[2] Sie teilt den Widerruf mittels Verfügung dem Betrieb und der Auftraggeberin mit.

[3] Wird die Betriebssicherheitserklärung widerrufen, so zieht die Auftraggeberin den Auftrag umgehend zurück; vorbehalten bleibt Artikel 58 Absatz 3. Der Betrieb hat keinen Anspruch auf Entschädigung.

6. Abschnitt: Wiederholung des Verfahrens und Rechtsschutz

Art. 68 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. 69 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 26 DSG[39].[40]

7. Abschnitt: Bearbeitung von Personendaten

Art. 70 Informationssystem zum Betriebssicherheitsverfahren

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

[2] Im Informationssystem können besonders schützenswerte Personendaten nach Artikel 5 Buchstabe c DSG[41] bearbeitet werden, sofern dies zur Durchführung des Betriebssicherheitsverfahrens erforderlich ist.[42]

[3] Das Informationssystem enthält folgende Daten:

a. die Daten nach den Artikeln 56 und 59 Absatz 3;

b. das Ergebnis der Beurteilung nach Artikel 55 Absatz 2;

c. die Ergebnisse der für das Betriebssicherheitsverfahren erforderlichen Personensicherheitsprüfungen nach Artikel 60 Absatz 1;

d. den Entscheid der Fachstelle BS nach Artikel 60 Absatz 2;

e. die Namen aller Betriebe mit einer Betriebssicherheitserklärung;

f. die Massnahmen allfälliger Kontrollen nach Artikel 64;

g. Daten und Akten aus Beschwerdeverfahren.

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

39 SR **235.1**
40 Fassung gemäss Anhang 2 Ziff. 5, in Kraft seit 1. Jan. 2024 (AS **2022** 232; **2023** 650; BBl **2017** 2953).
41 SR **235.1**
42 Fassung gemäss Anhang 2 Ziff. 5, in Kraft seit 1. Jan. 2024 (AS **2022** 232; **2023** 650; BBl **2017** 2953).

Art. 71 Zugriffsrechte und Datenbekanntgabe

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

a. Auftraggeberinnen: auf die Daten nach Artikel 70 Absatz 3 Buchstaben b und d–g;

b. betroffene Betriebe, sofern sie vom Bundesrat gestützt auf Artikel 31 Absatz 1 Buchstabe a ermächtigt worden sind, in ihrem Zuständigkeitsbereich Personensicherheitsprüfungen einzuleiten: auf die Daten nach Artikel 70 Absatz 3 Buchstabe d.

[2] Die Fachstelle BS kann zudem Daten nach Artikel 70 Absatz 3 Buchstaben b–d weiteren Stellen des Bundes bekanntgeben, sofern dies zur Gewährleistung der Informationssicherheit erforderlich ist.

Art. 72 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. 73

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 70;

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

5. Kapitel: Massnahmen des Bundes zum Schutz der Schweiz vor Cyberbedrohungen[43]

1. Abschnitt: Allgemeine Bestimmungen[44]

Art. 73*a*[45] Grundsatz

[1] Zum Schutz der Schweiz vor Cyberbedrohungen erstellt das BACS technische Analysen zur Bewertung und Abwehr von Cybervorfällen und Cyberbedrohungen sowie zur Identifikation und Behebung von Schwachstellen.

[2] Gestützt auf die Analysen nimmt das BACS insbesondere folgende Aufgaben wahr:

a. Sensibilisierung und Warnung der Öffentlichkeit in Bezug auf Cyberbedrohungen;

b. Warnung von betroffenen Behörden, Organisationen und Personen bei unmittelbaren Cyberbedrohungen oder laufenden Cyberangriffen;

c. Veröffentlichung von Informationen zur Cybersicherheit sowie von Empfehlungen für präventive und reaktive Massnahmen gegen Cybervorfälle;

d. Entgegennahme und Bearbeitung von Meldungen zu Cybervorfällen und Cyberbedrohungen;

e. Unterstützung von Betreiberinnen kritischer Infrastrukturen.

Art. 73*b*[46] Meldungen

[1] Das BACS nimmt Meldungen zu Cybervorfällen und Cyberbedrohungen entgegen. Die Meldungen können anonym erfolgen.

[2] Das BACS analysiert die Meldungen bezüglich ihrer Bedeutung für den Schutz der Schweiz vor Cyberbedrohungen. Es gibt auf Antrag eine Empfehlung zum weiteren Vorgehen ab, sofern dafür keine weiteren Analysen und Abklärungen erforderlich sind.

[3] Erhält das BACS Kenntnis von einer Schwachstelle, so informiert es umgehend die Herstellerin der betroffenen Hard- oder Software und setzt ihr zur Behebung der Schwachstelle eine angemessene Frist. Es weist sie darauf hin, dass eine Missachtung

43 Fassung gemäss Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

44 Eingefügt durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

45 Eingefügt durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

46 Eingefügt durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

beschaffungsrechtlich sanktioniert werden kann (Art. 44 Abs. 1 Bst. f^bis des Bundesgesetzes vom 21. Juni 2019[47] über das öffentliche Beschaffungswesen) und dass das BACS nach Fristablauf Informationen zur Schwachstelle nach Artikel 73*c* Absatz 2 veröffentlichen kann.

Art. 73*c*[48] Veröffentlichung von Informationen aus Meldungen

1 Das BACS kann Informationen zu Cybervorfällen veröffentlichen, sofern dies dem Schutz vor Cyberbedrohungen dient. Diese Informationen dürfen nur dann Aufschluss über die betroffene natürliche oder juristische Person geben, sofern diese einwilligt und es sich um missbräuchlich verwendete Identifikationsmerkmale und Adressierungselemente handelt.

2 Das BACS kann Informationen zu Schwachstellen unter Angabe der betroffenen Hard- oder Software veröffentlichen, sofern die Herstellerin einwilligt oder die Schwachstelle nicht innert der Frist nach Artikel 73*b* Absatz 3 behoben hat.

Art. 73*d*[49] Weiterleitung von Informationen

1 Das BACS kann Informationen aus Meldungen an Behörden und Organisationen weiterleiten, die im Bereich der Cybersicherheit tätig sind. Diese Informationen dürfen nur dann Personendaten umfassen, wenn die betroffene Person einwilligt.

2 Ergeben sich aus der Meldung eines Cybervorfalls oder dessen Analyse Informationen, die für das frühzeitige Erkennen und Verhindern von Bedrohungen der inneren oder äusseren Sicherheit, für die Beurteilung der Bedrohungslage oder für die nachrichtendienstliche Frühwarnung zum Schutz kritischer Infrastrukturen nach Artikel 6 Absätze 1 Buchstabe a, 2 und 5 des Nachrichtendienstgesetzes vom 25. September 2015[50] (NDG) erforderlich sind, so leitet das BACS diese Informationen an den NDB weiter.

3 Erhalten Mitarbeiterinnen und Mitarbeiter des BACS im Zusammenhang mit einer Meldung oder deren Analyse Hinweise auf eine mögliche Straftat, so zeigen sie diese abweichend von Artikel 22*a* Absatz 1 des Bundespersonalgesetzes vom 24. März 2000[51] ausschliesslich der Leiterin oder dem Leiter des BACS an. Diese oder dieser kann Anzeige bei den Strafverfolgungsbehörden erstatten, sofern dies aufgrund der Schwere der möglichen Straftat geboten scheint.

4 Strafrechtlich geschützte Geheimnisse darf das BACS nur nach den Vorgaben von Artikel 320 des Strafgesetzbuches[52] weiterleiten.

47 SR **172.056.1**
48 Eingefügt durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).
49 Eingefügt durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).
50 SR **121**
51 SR **172.220.1**
52 SR **311.0**

Art. 74[53] Unterstützung von Betreiberinnen kritischer Infrastrukturen

[1] Das BACS unterstützt die Betreiberinnen kritischer Infrastrukturen beim Schutz vor Cyberbedrohungen.

[2] Es stellt ihnen insbesondere folgende Hilfsmittel unentgeltlich und zur freiwilligen Nutzung zur Verfügung:

a. ein Kommunikationssystem für den sicheren Informationsaustausch;

b. technische Informationen zu aktuellen Cyberbedrohungen sowie Empfehlungen für präventive und reaktive Massnahmen gegen Cybervorfälle;

c. technische Instrumente und Anleitungen zur Erkennung von Cybervorfällen, die auf den erhöhten Schutzbedarf kritischer Infrastrukturen ausgerichtet sind.

[3] Es kann sie bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen beraten und unterstützen, wenn die Funktionsfähigkeit der betroffenen kritischen Infrastruktur gefährdet ist und, sofern es sich um private Betreiberinnen handelt, die Beschaffung gleichwertiger Unterstützung auf dem Markt nicht rechtzeitig möglich ist.

[4] Es kann zur Analyse eines Cybervorfalls mit dem Einverständnis der betroffenen Betreiberin auf deren Informationen und Informatikmittel zugreifen.

2. Abschnitt:[54] Pflicht zur Meldung von Cyberangriffen

Art. 74*a* Grundsätze

[1] Behörden und Organisationen nach Artikel 74*b* müssen dafür sorgen, dass dem BACS Cyberangriffe auf ihre Informatikmittel gemeldet werden.

[2] Das BACS erteilt interessierten Behörden und Organisationen Auskunft darüber, ob sie der Meldepflicht unterstellt sind und erlässt auf Antrag eine entsprechende Verfügung.

[3] Durch die Meldung eines Cyberangriffs haben die meldepflichtigen Behörden und Organisationen Anspruch auf die Unterstützung des BACS bei der Vorfallbewältigung nach Artikel 74 Absatz 3.

[4] Die Meldepflicht dient ausschliesslich dazu, dass das BACS Angriffsmuster auf kritische Infrastrukturen frühzeitig erkennen und dadurch mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

53 Fassung gemäss Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

54 Eingefügt durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

Art. 74*b* Meldepflichtige Behörden und Organisationen

[1] Die Meldepflicht gilt für:

a. Hochschulen nach Artikel 2 Absatz 2 des Hochschulförderungs- und -koordinationsgesetzes vom 30. September 2011[55];

b. Bundes-, Kantons- und Gemeindebehörden sowie interkantonale, kantonale und interkommunale Organisationen, mit Ausnahme der Gruppe Verteidigung, wenn die Armee Assistenzdienst nach Artikel 67 oder Aktivdienst nach Artikel 76 des Militärgesetzes vom 3. Februar 1995[56] leistet;

c. Organisationen mit öffentlich-rechtlichen Aufgaben in den Bereichen Sicherheit und Rettung, Trinkwasserversorgung, Abwasseraufbereitung und Abfallentsorgung;

d. Unternehmen, die in den Bereichen Energieversorgung nach Artikel 6 Absatz 1 des Energiegesetzes vom 30. September 2016[57], Energiehandel, Energiemessung oder Energiesteuerung tätig sind, mit Ausnahme der Bewilligungsinhaber gemäss Kernenergiegesetz vom 21. März 2003[58], sofern ein Cyberangriff auf eine Kernanlage erfolgt;

e. Unternehmen, die dem Bankengesetz vom 8. November 1934[59], dem Versicherungsaufsichtsgesetz vom 17. Dezember 2004[60] oder dem Finanzmarktinfrastrukturgesetz vom 19. Juni 2015[61] unterstehen;

f. Gesundheitseinrichtungen, die auf der kantonalen Spitalliste nach Artikel 39 Absatz 1 Buchstabe e des Bundesgesetzes vom 18. März 1994[62] über die Krankenversicherung aufgeführt sind;

g. medizinische Laboratorien mit einer Bewilligung nach Artikel 16 Absatz 1 des Epidemiengesetzes vom 28. September 2012[63];

h. Unternehmen, die für die Herstellung, das Inverkehrbringen und die Einfuhr von Arzneimitteln eine Bewilligung nach dem Heilmittelgesetz vom 15. Dezember 2000[64] haben;

i. Organisationen, die Leistungen zur Absicherung gegen die Folgen von Krankheit, Unfall, Arbeits- und Erwerbsunfähigkeit, Alter, Invalidität und Hilflosigkeit erbringen;

j. die Schweizerische Radio- und Fernsehgesellschaft;

k. Nachrichtenagenturen von nationaler Bedeutung;

55 SR **414.20**
56 SR **510.10**
57 SR **730.0**
58 SR **732.1**
59 SR **952.0**
60 SR **961.01**
61 SR **958.1**
62 SR **832.10**
63 SR **818.101**
64 SR **812.21**

l. Anbieterinnen von Postdiensten, die nach Artikel 4 Absatz 1 des Postgesetzes vom 17. Dezember 2010[65] bei der Postkommission registriert sind;

m. Eisenbahnunternehmen nach Artikel 5 oder 8*c* des Eisenbahngesetzes vom 20. Dezember 1957[66] sowie Seilbahn-, Trolleybus-, Autobus- und Schifffahrtsunternehmen mit einer Konzession nach Artikel 6 des Personenbeförderungsgesetzes vom 20. März 2009[67];

n. Unternehmen der Zivilluftfahrt, die über eine Bewilligung des Bundesamtes für Zivilluftfahrt verfügen, sowie die Landesflughäfen gemäss Sachplan Infrastruktur der Luftfahrt;

o. Unternehmen, die nach dem Seeschifffahrtsgesetz vom 23. September 1953[68] Güter auf dem Rhein befördern, sowie Unternehmen, welche die Registrierung, Ladung oder Löschung im Hafen Basel betreiben;

p. Unternehmen, welche die Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs versorgen und deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen führen würde;

q. Anbieterinnen von Fernmeldediensten, die beim Bundesamt für Kommunikation nach Artikel 4 Absatz 1 FMG[69] registriert sind;

r. Registerbetreiberinnen und Registrare von Internet-Domains nach Artikel 28*b* FMG;

s. Anbieterinnen und Betreiberinnen von Diensten und Infrastrukturen, die der Ausübung der politischen Rechte dienen;

t. Anbieterinnen und Betreiberinnen von Cloudcomputing, Suchmaschinen, digitalen Sicherheits- und Vertrauensdiensten sowie Rechenzentren, sofern sie einen Sitz in der Schweiz haben;

u. Herstellerinnen von Hard- oder Software, deren Produkte von kritischen Infrastrukturen genutzt werden, sofern die Hard- oder Software einen Fernwartungszugang hat oder zu einem der folgenden Zwecken eingesetzt wird:

1. Steuerung und Überwachung von betriebstechnischen Systemen und Prozessen,
2. Gewährleistung der öffentlichen Sicherheit.

[2] Bei Behörden und Organisationen, die auch Tätigkeiten ausüben, die nicht unter Absatz 1 fallen, besteht keine Meldepflicht für Cyberangriffe, die sich ausschliesslich auf diese Tätigkeiten auswirken.

[3] Die Meldepflicht nach Absatz 1 gilt für Cyberangriffe, die sich in der Schweiz auswirken, auch wenn sich die betroffenen Informatikmittel im Ausland befinden.

65 SR **783.0**
66 SR **742.101**
67 SR **745.1**
68 SR **747.30**
69 SR **784.10**

Art. 74*c* Ausnahmen von der Meldepflicht

Der Bundesrat nimmt Behörden und Organisationen von der Meldepflicht nach Artikel 74*b* aus, wenn durch Cyberangriffe ausgelöste Funktionsstörungen nur geringe Auswirkungen auf das Funktionieren der Wirtschaft oder das Wohlergehen der Bevölkerung haben.

Art. 74*d* Zu meldende Cyberangriffe

Ein Cyberangriff muss gemeldet werden, wenn er:

a. die Funktionsfähigkeit der betroffenen kritischen Infrastruktur gefährdet;

b. zu einer Manipulation oder zu einem Abfluss von Informationen geführt hat;

c. über einen längeren Zeitraum unentdeckt blieb, insbesondere wenn Anzeichen dafür bestehen, dass er zur Vorbereitung weiterer Cyberangriffe ausgeführt wurde; oder

d. mit Erpressung, Drohung oder Nötigung verbunden ist.

Art. 74*e* Frist und Inhalt der Meldung

1 Die Meldung muss innert 24 Stunden nach der Entdeckung des Cyberangriffs erfolgen.

2 Sie muss Informationen zur meldepflichtigen Behörde oder Organisation, zur Art und Ausführung des Cyberangriffs, zu seinen Auswirkungen, zu ergriffenen Massnahmen und, soweit bekannt, zum geplanten weiteren Vorgehen enthalten.

3 Sind zum Zeitpunkt der Meldung nicht alle erforderlichen Informationen bekannt, so ergänzt die meldepflichtige Behörde oder Organisation die Meldung, sobald sie über neue Informationen verfügt.

4 Wer die Meldepflicht für eine Behörde oder Organisation zu erfüllen hat, muss im Rahmen der Meldung keine Angaben machen, die sie oder ihn strafrechtlich belasten.

5 Das BACS informiert die meldepflichtige Behörde oder Organisation, sobald alle Angaben zur Erfüllung der Meldepflicht vorliegen.

Art. 74*f* Übermittlung der Meldung

1 Für die elektronische Meldung von Cyberangriffen stellt das BACS ein sicheres System zur Übermittlung der Meldung zur Verfügung.

2 Das System muss den meldepflichtigen Behörden und Organisationen ermöglichen, die Meldung des Cyberangriffs oder seiner Auswirkungen gesamthaft oder in Teilen an weitere Behörden zu übermitteln.

3 Sind zur Erfüllung einer Meldepflicht gegenüber weiteren Behörden Informationen erforderlich, die über Artikel 74*e* hinausgehen, so muss das System den meldepflichtigen Behörden und Organisationen ermöglichen, diese Informationen direkt an die betreffenden Behörden zu übermitteln, ohne dass das BACS darauf Zugriff hat.

3. Abschnitt: Datenschutz und Informationsaustausch[70]

Art. 75[71] Bearbeitung von Personendaten

[1] Das BACS kann zur Erfüllung seiner Aufgaben Personendaten bearbeiten, einschliesslich Adressierungselemente nach Artikel 3 Buchstabe f FMG[72] und damit zusammenhängende besonders schützenswerte Personendaten, die Informationen enthalten über:

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

b. administrative oder strafrechtliche Verfolgungen und Sanktionen.

[2] Bei der Bearbeitung von Personendaten oder bei konkreten Hinweisen auf den Missbrauch einer Identität oder auf die unberechtigte Verwendung von Adressierungselementen informiert das BACS die betroffenen Personen, sofern dies nicht mit unverhältnismässigem Aufwand verbunden ist und keine überwiegenden öffentlichen Interessen entgegenstehen.

Art. 76[73] Zusammenarbeit im Inland

[1] Das BACS und die Betreiberinnen kritischer Infrastrukturen können Personendaten untereinander austauschen, sofern dies zum Schutz vor Cyberbedrohungen erforderlich ist.

[2] Das BACS und die Fernmeldedienstanbieterinnen können Adressierungselemente und damit zusammenhängende Personendaten untereinander austauschen, sofern dies zum Schutz vor Cyberbedrohungen erforderlich ist.

Art. 76*a*[74] Unterstützung für Behörden

[1] Das BACS unterstützt den NDB mit periodischen Auswertungen zu Anzahl, Art und Ausmass von Cyberangriffen sowie, auf Anfrage, mit technischen Analysen von Cyberbedrohungen.

70 Eingefügt durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).
71 Fassung gemäss Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).
72 SR **784.10**
73 Fassung gemäss Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).
74 Eingefügt durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

2 Es gewährt dem NDB zum Zweck des frühzeitigen Erkennens und Verhinderns von Bedrohungen der inneren oder äusseren Sicherheit, zur Beurteilung der Bedrohungslage und zur nachrichtendienstlichen Frühwarnung zum Schutz kritischer Infrastrukturen nach Artikel 6 Absätze 1 Buchstabe a, 2 und 5 NDG[75] Zugriff auf Informationen, welche die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen betreffen.

3 Es gewährt den Strafverfolgungsbehörden Zugriff auf Informationen, welche die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen betreffen.

4 Es gewährt den kantonalen Stellen, die für die Cybersicherheit zuständig sind, Zugriff auf Informationen, die für den Schutz vor Cyberbedrohungen erforderlich sind.

Art. 77[76] Internationale Zusammenarbeit

1 Das BACS kann mit ausländischen und internationalen Stellen, die für die Cybersicherheit zuständig sind, Informationen austauschen, die Aufschluss über die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen geben, wenn sie diese zur Erfüllung von Aufgaben benötigen, die denjenigen des BACS entsprechen. Umfasst der Informationsaustausch auch Personendaten, sind Artikel 16 und 17 DSG[77] zu beachten.

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

Art. 78[78]

Art. 79 Datenaufbewahrung und -archivierung

1 Das BACS bewahrt Personendaten nur so lange auf, wie dies zur Erkennung von Cyberbedrohungen oder zur Bewältigung von Cybervorfällen zweckmässig ist, höchstens jedoch fünf Jahre ab der letzten Verwendung zu diesem Zweck. Bei besonders schützenswerten Personendaten beträgt die Frist zwei Jahre.[79]

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

75 SR **121**
76 Fassung gemäss Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).
77 SR **235.1**
78 Aufgehoben durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), mit Wirkung seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).
79 Fassung gemäss Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), in Kraft seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

Art. 80[80]

6. Kapitel: Organisation und Vollzug

1. Abschnitt: Organisation

Art. 81 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 74 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. 82 Konferenz der Informationssicherheitsbeauftragten

[1] Die Konferenz der Informationssicherheitsbeauftragten wird aus den Informationssicherheitsbeauftragten nach Artikel 81 Absatz 1 sowie zwei Vertreterinnen oder Vertretern der Kantone und der oder dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gebildet.

80 Aufgehoben durch Ziff. I des BG vom 29. Sept. 2023 (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), mit Wirkung seit 1. April 2025 (AS **2024** 257; **2025** 173; BBl **2023** 84).

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 85 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. 83 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. 84 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. 85 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. 86 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. 87 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. 88 Evaluation

[1] Der Bundesrat sorgt dafür, dass die Umsetzung, die Zweckmässigkeit, die Wirksamkeit und die Wirtschaftlichkeit dieses Gesetzes periodisch durch eine unabhängige Stelle, wie die Eidgenössische Finanzkontrolle, überprüft werden.

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

7. Kapitel: Schlussbestimmungen

Art. 89 Änderung anderer Erlasse

Die Änderung anderer Erlasse wird im Anhang 1 geregelt.

Art. 90 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. 91 Koordination mit anderen Erlassen

Die Koordination mit anderen Erlassen wird im Anhang 2 geregelt.

Art. 92 Referendum und Inkrafttreten

[1] Dieses Gesetz untersteht dem fakultativen Referendum.

[2] Der Bundesrat bestimmt das Inkrafttreten.

Datum des Inkrafttretens:
Artikel 87: 1. Mai 2022[81]
Die übrigen Bestimmungen: 1. Januar 2024[82]

81 BRB vom 6. April 2022
82 V vom 8. Nov. 2023 (AS **2023** 650)

Anhang 1
(Art. 89)

Änderung anderer Erlasse

Die nachstehenden Erlasse werden wie folgt geändert:

…[83]

83 Die Änderungen können unter AS **2022** 232 konsultiert werden.

Anhang 2
(Art. 91)

Koordination anderer Erlasse

…[84]

84 Die Koordinationbestimmungen können unter AS **2022** 232 konsultiert werden.