Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Generalsekretariat VBS GS-VBS
Digitalisierung und Cybersicherheit VBS

24. August 2022

Ausführungsrecht zum Informationssicherheitsgesetz

Erläuternder Bericht

Aktenzeichen: GS-VBS-251.2-35/1/6/8

Übersicht

Am 18. Dezember 2020 hat die Bundesversammlung das Informationssicherheitsgesetz (ISG) verabschiedet. Das neue Gesetz schafft einen einheitlichen formell-gesetzlichen Rahmen für die Informationssicherheit beim Bund.

Die vorliegenden Ausführungserlasse zum ISG wurden in Zusammenarbeit mit Vertreterinnen und Vertretern der anderen Bundesbehörden und der Kantone erarbeitet. In der Botschaft vom 22. Februar 2017 zum Informationssicherheitsgesetz hat der Bundesrat angekündigt, dass er die anderen Bundesbehörden und die Kantone für alle wichtigen Regelungen zur Stellungnahme einladen würde. So soll einerseits ein möglichst einheitliches Sicherheitsniveau erreicht und andererseits den Bedürfnissen aller Bundesbehörden sowie der Kantone gebührend Rechnung getragen werden. Deshalb wird ein Vernehmlassungsverfahren durchgeführt.

Das Ausführungsrecht zum ISG umfasst insgesamt drei neue Verordnungen und eine Änderung einer bestehenden Verordnung:

- Informationssicherheitsverordnung: Die neue Verordnung regelt das Management der Informationssicherheit, den Schutz von klassifizierten Informationen, die Informatiksicherheit und die Massnahmen zur personellen und physischen Sicherheit für die Bundesverwaltung und die Armee. Sie legt die entsprechenden Aufgaben, Kompetenzen und Verantwortlichkeiten fest. Die wichtigste Änderung ist die Einführung eines Informationssicherheits-Managementsystems bei allen Verwaltungseinheiten;
- Verordnung über die Personensicherheitsprüfungen: Die neue Verordnung fasst die Ausführungsbestimmungen zu den verschiedenen Personensicherheitsprüfungen zusammen. Diese Prüfungen werden auf das Mindestmass reduziert, das zur Identifizierung von erheblichen Risiken für den Bund erforderlich ist. Damit werden künftig deutlich weniger Prüfungen durchgeführt;
- Verordnung über das Betriebssicherheitsverfahren: Die neue Verordnung regelt die Einzelheiten des durch das ISG eingeführten Betriebssicherheitsverfahrens. Das Betriebssicherheitsverfahren ist auf alle sicherheitsempfindlichen Aufträge anwendbar, die der Bund vergibt;
- Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes: Die Teilrevision dieser Verordnung beinhaltet nebst vorwiegend technischen Anpassungen eine Erweiterung des Geltungsbereichs der Verordnung auf die Verwaltungseinheiten der dezentralen Bundesverwaltung.

Das Inkrafttreten des ISG und der Ausführungsbestimmungen ist auf Mitte 2023 geplant.

Inhaltsverzeichnis

Erläuternder Bericht

1 Ausgangslage

Am 18. Dezember 2020 hat die Bundesversammlung das Informationssicherheitsgesetz (ISG) verabschiedet.[1] Die Referendumsfrist ist Mitte April 2021 unbenutzt abgelaufen. Das neue Gesetz schafft einen einheitlichen formell-gesetzlichen Rahmen für die Informationssicherheit beim Bund.

Der Begriff «Informationssicherheit» umfasst die Gesamtheit aller Anforderungen und Massnahmen, mit denen die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Nachvollziehbarkeit von Informationen und Daten aller Art sowie die Verfügbarkeit und die Integrität von Informatikmitteln geschützt werden. Da Informationen heute mehrheitlich elektronisch bearbeitet werden, wird ein Schwergewicht auf die «Cybersicherheit» gelegt. Der Begriff «Informationssicherheit» umfasst aber alle Bearbeitungsvorgänge, also auch Papierdokumente und mündliche Äusserungen, und nicht nur die elektronische Bearbeitung. Umgangssprachlich werden beide Begriffe dennoch oft als Synonym verwendet.

Die vorliegenden Ausführungserlasse zum ISG wurden in Zusammenarbeit mit Vertreterinnen und Vertretern der anderen Bundesbehörden und der Kantone erarbeitet. In seiner Botschaft vom 22. Februar 2017[2] zum Informationssicherheitsgesetz (ISG-Botschaft) hat der Bundesrat angekündigt, dass er die anderen Bundesbehörden und die Kantone für alle wichtigen Regelungen zur Stellungnahme einladen würde (Vgl. Ziff. 1.5, S. 3009). So kann einerseits ein möglichst einheitliches Sicherheitsniveau erreicht und andererseits den Bedürfnissen aller Bundesbehörden sowie der Kantone gebührend Rechnung getragen werden. Deshalb wird ein Vernehmlassungsverfahren durchgeführt.

2 Rechtsvergleich, insbesondere mit dem europäischen Recht

In vielen Ländern aus dem europäischen Umfeld werden die Rechtsgrundlagen zur Informationssicherheit an die neue Realität der Informationsgesellschaft angepasst. Aufgrund der teilweise sehr unterschiedlichen Rechtsordnungen und staatlichen Grundstrukturen können die entsprechenden Regelungen in Bezug auf Normenhierarchie und Geltungsbereich kaum verglichen werden. Hingegen kann festgehalten werden, dass die Bestimmungen des ISG und seiner Ausführungserlasse grundsätzlich mit den Regelungen der verglichenen Staaten entweder übereinstimmen oder zumindest harmonisiert sind. Im organisatorischen Bereich wird der Bund mit der Fachstelle des Bundes für Informationssicherheit über eine einzige Anlaufstelle im internationalen Verhältnis verfügen. Dadurch soll die internationale Zusammenarbeit im Bereich der Informationssicherheit einfacher und effizienter werden.

3 Grundzüge der Vorlagen

3.1 Umfang des Ausführungsrechts zum ISG

Das Ausführungsrecht zum ISG umfasst vier Verordnungen:

- eine neue Informationssicherheitsverordnung (ISV, vgl. Ziff. 3.3);
- eine Änderung der bestehenden Verordnung vom 19. Oktober 2016[3] über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV, vgl. Ziff. 3.4);
- eine neue Verordnung über die Personensicherheitsprüfungen (VPSP, vgl. Ziff. 3.5);
- eine neue Verordnung über das Betriebssicherheitsverfahren (VBSV, vgl. Ziff. 3.6).

Der Bundesrat hat am 12. Januar 2022 die Vernehmlassung zur Vorlage für die Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen eröffnet. Die Einführung einer solchen Meldepflicht bedingt die vollständige Überarbeitung des 5. Kapitels des ISG. Diese Revision des ISG samt Verordnung soll Ende 2023 in Kraft treten. Daher ist es nicht zielführend, eine neue Verordnung für den heutigen Bedarf zu verabschieden, die wenige Monate später bereits totalrevidiert wird. Aus diesem Grund wird vorerst auf den Erlass von Ausführungsbestimmungen zum 5. Kapitel des ISG verzichtet.

[1] BBl **2020** 9975
[2] BBl **2017** 2953
[3] SR **172.010.59**

3.2 Rahmenbedingungen und Grundsätze

Der Bundesrat hat in der ISG-Botschaft die formelle und materielle Notwendigkeit des ISG begründet. Diese Ausgangslage und die damit verbundenen Ziele und Lösungsansätze des Bundesrats haben an Aktualität nicht verloren. Sie dienen als konzeptionelle Grundlage für das Ausführungsrecht zum ISG. Dasselbe gilt für die Beurteilung der Bedrohung, die strategische Ausrichtung der Schweiz sowie die Handlungsgrundsätze, die der Bundesrat am 18. April 2018 in der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022 festgelegt hat. Für die Umsetzung der Informationssicherheit in der Bundesverwaltung und in der Armee sind weitere Strategien zu berücksichtigen, insbesondere die nationalen und bundesinternen Informatikstrategien.

Für die Erarbeitung des Ausführungsrechts zum ISG wurden die nachfolgenden fünf Grundsätze als strategische Wegweiser definiert:

a. Vernetzte Sicherheitsverantwortung

Die Direktorinnen und Direktoren der Verwaltungseinheiten sind gemäss Artikel 45 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[4] (RVOG) für die Erfüllung der ihnen übertragenen Aufgaben, einschliesslich des Schutzes ihrer Informationen und Informatikmittel, verantwortlich. In einem vernetzten, digitalisierten Umfeld genügt diese isoliert betrachtete Verantwortung jedoch nicht. Informationen werden ausgetauscht, Systeme vernetzt und Datensammlungen nach dem sogenannten «Once-Only-Prinzip» zur geteilten Nutzung bereitgestellt. Dadurch können sich Bedrohungen und Angriffe gegen eine Organisation oder deren Lieferanten auch auf den Zuständigkeitsbereich anderer Organisationen erstrecken. Die Informationssicherheit ist deshalb zwangsläufig eine vernetzte Aufgabe mit vernetzter Verantwortung, welche gemeinsame Ziele, ein koordiniertes Vorgehen und Minimalstandards verlangt.

b. Risikobasierter Ansatz

Eine absolute Sicherheit ist bekanntlich nicht erreichbar. Risiken sind daher unvermeidbar. Die Grundschutzvorgaben des Bundes bieten einen risikogerechten Schutz gegen eine Vielzahl von Bedrohungen. Sie dienen der vernetzten Informationssicherheit des Bundes und müssen eingehalten werden. Ergänzend müssen die Verantwortlichen im Bereich der Informationssicherheit ein aktives Risikomanagement betreiben, in dessen Rahmen Schwachstellen und Bedrohungen und deren potenziellen Auswirkungen auf die Aufgabenerfüllung bewusst berücksichtigt und priorisiert werden. So entsteht eine angemessene Sicherheit. Mit solch einem risikobasierten Ansatz kann der Fokus neben den Risiken auch auf Möglichkeiten und Chancen, neue Ideen, Anwendungen oder Technologien gerichtet werden.

c. Harmonisierung und Standardisierung

Eine angemessene Informationssicherheit ist eine Voraussetzung für das Vertrauen in E-Government. Dies gilt nicht nur für den inländischen Bereich, sondern auch für die zunehmende internationale Behördenvernetzung. Eine nationale und internationale Harmonisierung der Vorschriften und Standardisierung der Sicherheitsmassnahmen ist deshalb anzustreben. Die Standardisierung hat weitere wichtige Vorteile: Zum einen werden den Entwicklungs- und Beschaffungsstellen klare Sicherheitsanforderungen vorgelegt, die sie bei der Implementierung der Sicherheit in die Informatikmittel unterstützen. Zum anderen werden die Sicherheitskosten in Projekten berechen- und planbarer.

d. Technologieneutralität

Mit zunehmender Digitalisierung entstehen stets neue sicherheitsrelevante Technologien, Konzepte oder Arbeitsformen. Das Verordnungsrecht muss in der Lage sein, Entwicklungen wie «Cloud-Computing», «Internet of Things», «künstliche Intelligenz» oder «Quantum-Computing» zu berücksichtigen, ohne ständig angepasst werden zu müssen. Deshalb sollen auf Verordnungsebene in erster Linie Grundsätze, Aufgaben, Kompetenzen und Verantwortlichkeiten festgelegt werden. Technologiebedingte Vorgaben sollen auf Stufe der technischen Weisungen und Standards definiert werden.

[4] SR **172.010**

e. Digitalisierung ermöglichen

Bei den Rechtsetzungsprojekten müssen die Bedürfnisse der Digitalisierung frühzeitig berücksichtigt werden. Wenn Aufgaben, Prozesse und Verfahren rechtlich überprüft oder neu definiert werden, muss sichergestellt werden, dass die neuen Vorschriften die Digitalisierung ermöglichen.

3.3 Informationssicherheitsverordnung (ISV)

a. Gegenstand

Die neue Informationssicherheitsverordnung (ISV) ersetzt die bisherige Cyberrisikenverordnung vom 27. Mai 2020[5] (CyRV) und Informationsschutzverordnung vom 4. Juli 2007[6] (ISchV). Die ISV regelt das Management der Informationssicherheit, den Schutz von klassifizierten Informationen, die Informatiksicherheit und die Massnahmen zur personellen und physischen Sicherheit. Sie legt die entsprechenden Aufgaben, Kompetenzen und Verantwortlichkeiten in der Bundesverwaltung und in der Armee fest.

b. Geltungsbereich

Die ISV gilt für den Bundesrat, die Bundesverwaltung und die Armee. Die Verwaltungseinheiten der dezentralen Bundesverwaltung nach Artikel 7a der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[7] (RVOV) werden der ISV nur unterstellt, wenn ihre Aufgaben sicherheitsempfindlich sind oder ein erhebliches Risiko für die zentrale Bundesverwaltung darstellen können. Diese Voraussetzungen sind erfüllt, wenn die dezentralen Verwaltungseinheiten auf Informatikmittel der zentralen Bundesverwaltung der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz» zugreifen, wenn sie selber solche Informatikmittel einsetzen oder wenn sie klassifizierte Informationen des Bundes bearbeiten. Die BK und die Departemente können beim Bundesrat zudem beantragen, weitere dezentrale Verwaltungseinheiten zu unterstellen.

Organisationen nach Artikel 2 Absatz 4 RVOG, die mit Verwaltungsaufgaben betraut werden aber nicht der Bundesverwaltung angehören, werden vollständig vom Geltungsbereich des ISG – und demzufolge auch der ISV – ausgenommen. Sie gelten als Dritte.

Die ISV gilt sinngemäss für die Bundesversammlung, die eidgenössischen Gerichte, die Schweizerische Bundesanwaltschaft und ihre Aufsichtsbehörde sowie die Schweizerische Nationalbank, wenn sie keine eigenen Vorschriften erlassen.

c. Zusammenarbeit mit den Kantonen

Sofern die Kantone klassifizierte Informationen des Bundes bearbeiten, gelten die entsprechenden Vorschriften des ISG und der ISV. Wenn sie auf Informatikmittel des Bundes zugreifen, gelten für sie die Vorgaben des ISG und der ISV über die Informatiksicherheit. In der Praxis werden die Kantone wie heute die Sicherheitsanforderungen erfüllen müssen, die das für das Informatikmittel verantwortliche Bundesamt in Anwendung der Vorgaben des ISG und der ISV festgelegt hat. Die Kantone können sich allerdings von den bundesrechtlichen Vorgaben befreien, wenn sie von sich aus eine gleichwertige Informationssicherheit gewährleisten. Dies setzt voraus, dass sie eigene, an den Bundesstandard angeglichene Sicherheitsvorschriften erlassen, die sie in ihrem Zuständigkeitsbereich durchsetzen. Massgebende Bundestandards sind die Vorschriften und technischen Anforderungen für den Grundschutz der Informatik im Bund sowie für den Schutz von klassifizierten Informationen. Die Kantone sind nicht verpflichtet, ein Informationssicherheits-Managementsystem (ISMS) umzusetzen.

d. Management der Informationssicherheit

Sämtliche Verwaltungseinheiten werden verpflichtet, ihre Informationssicherheit mittels eines Informationssicherheits-Managementsystems (ISMS) umzusetzen. Ein ISMS ist ein Führungsinstrument und dient der systematischen Planung, Umsetzung, Überprüfung und Verbesserung der Informationssicherheit. Es umfasst die dafür nötigen Vorschriften und Verfahren und macht sichtbar, wem in der Organisation, welche Aufgaben, Kompetenzen und Verantwortlichkeiten zugeordnet werden. Mit dem Begriff «ISMS» wird implizit auf die Norm ISO/IEC 27001 verwiesen, die sowohl in der Privatwirtschaft als auch vermehrt in öffentlichen Verwaltungen als Standard gilt. Mehrere Verwaltungseinheiten und Departemente haben sich bereits entschieden, ihre Informationssicherheit systematisch nach der ISO-Norm umzusetzen. Einige davon sind formell zertifiziert. Von

[5] SR **120.73**
[6] SR **510.411**
[7] SR **172.010.1**

den Verwaltungseinheiten verlangt die ISV lediglich ein ISMS «*light*»: Das heisst, sie müssen nicht die vollständige ISO-Norm, sondern nur die wichtigsten Managementprozesse umsetzen. Diese sind in der ISV aufgeführt. Eine externe Zertifizierung wird nicht verlangt. Die Verwaltungseinheiten und Departemente können allerdings ein höheres Ambitionsniveau festlegen.

e. Schutz von klassifizierten Informationen und Informatiksicherheit

Die Kriterien zur Klassifizierung von Informationen und zur Sicherheitseinstufung von Informatikmitteln werden an die Massstäbe des Risikomanagements Bund angeglichen. Diese Kriterien sind von Natur aus schwammig und müssen ausgelegt werden. Für die Umsetzung werden Hilfsmittel erstellt. Inskünftig wird der Bund weniger klassifizieren.

Bei den konkreten Massnahmen zum Schutz von klassifizierten Informationen und zur Gewährleistung der Informatiksicherheit übernimmt die ISV mehrheitlich die bestehenden Regelungen der ISchV und CyRV. Die detaillierten Vorgaben, einschliesslich der derzeit fehlenden technischen Anforderungen an die elektronische Bearbeitung von klassifizierten Informationen, werden voraussichtlich bis Ende 2023 erarbeitet und, wo möglich und sinnvoll, an internationale Standards angeglichen.

f. Sicherheitsakkreditierung von Informatikmitteln

Neu führt die ISV für eine beschränkte Anzahl sicherheitsempfindlicher Informationssysteme, in welchen VERTRAULICH oder GEHEIM klassifizierte Informationen bearbeitet werden (beispielsweise eine Anwendung für die vertrauliche Videokommunikation), eine Akkreditierungspflicht ein. Die ISV schliesst damit eine Lücke, welche heute die internationale Zusammenarbeit im Sicherheitsbereich erschwert. Eine Sicherheitsakkreditierung wird im Ausland und in der internationalen Zusammenarbeit verlangt, wenn geschützte Informationen einer Behörde (oder eines Staates) in einem System einer anderen Behörde (oder eines anderen Staates) bearbeitet werden sollen. Diese belegt, dass das Empfängersystem die vorgegebenen Sicherheitsanforderungen erfüllt und die Restrisiken nach dem Stand der Technik tragbar sind. Kann die Sicherheitsakkreditierung nicht erteilt werden, so soll der Bundesrat die Restrisiken beurteilen und über den Einsatz des Informatikmittels entscheiden.

g. Personensicherheit

Die Wahrnehmung der Verantwortung für die personenbezogenen Sicherheitsrisiken ist eine ständige Führungsaufgabe. Der neu mit dem ISG eingeführte Artikel 20*a* des Bundespersonalgesetzes[8] vom 24. März 2000 (BPG) ermächtigt die Verwaltungseinheiten, von Bewerbenden und von Angestellten einen Auszug aus dem Strafregister und aus dem Betreibungsregister zu verlangen, wenn dies zur Wahrung ihrer Interessen erforderlich ist. Die Praxis hat gezeigt, dass personenbezogene Sicherheitsrisiken nach bestandener Personensicherheitsprüfung (PSP) eher selten wieder thematisiert werden. Im Sinne einer international üblichen Nachsorge (sogenanntes «aftercare») sollen sicherheitsgeprüfte Mitarbeitende ihrem Arbeitgeber deshalb Umstände aus ihrem privaten und beruflichen Umfeld, welche die Sicherheit gefährden können, melden müssen (z. B. Erpressbarkeit aufgrund grosser Verschuldung im Spielcasino). Der Umgang mit einem allenfalls erhöhten Risiko ist Sache des Arbeitgebers. Dieser kann von den betroffenen Mitarbeitenden auch während der Wiederholungsfrist der PSP Auszüge nach Artikel 20*a* BPG verlangen. Je nach Einzelfall kann eine solche Meldung auch zu einer ausserordentlichen Wiederholung der PSP führen.

h. Sicherheitsverantwortliche und Informationssicherheitsbeauftragte

Eine wichtige Neuerung in der ISV betrifft die Amtsleitungen. Ihnen werden in der ISV konkrete Aufgaben, Kompetenzen und Verantwortlichkeiten im Bereich Informationssicherheit übertragen, die sie bei Bedarf an ein Mitglied ihrer Geschäftsleitung delegieren dürfen (Sicherheitsverantwortliche). Die Sicherheitsverantwortlichen beaufsichtigen das ISMS des Amts und treffen alle wichtigen Entscheide im Bereich Informationssicherheit. Die operativen Aufsichtstätigkeiten sind Aufgabe der Informationssicherheitsbeauftragten gemäss Artikel 37. Mit der ISV werden die heutigen Rollen der «Informatiksicherheitsbeauftragten» und der «Informationsschutzbeauftragten» in der neuen Rolle der «Informationssicherheitsbeauftragten» vereint. Ihre Aufgaben werden entsprechend präzisiert und mit dem Betrieb des ISMS ergänzt.

[8] SR **172.220.1**

Die Departemente sind im Sinne der Artikel 37–38 und 41–42 RVOG für die Steuerung, Koordination und Überwachung der Informationssicherheit im Departement verantwortlich. Sie bestimmen insbesondere die Informationssicherheitspolitik und die Sicherheitsorganisation des Departements. Die operative Verantwortung für die Sicherheit soll von der Generalsekretärin oder dem Generalsekretär getragen werden, sofern die Departementsvorsteherin oder der Departementsvorsteher nicht anders entscheidet. Die Informationssicherheitsbeauftragten nehmen wie bis anhin die operativen Koordinations- und Aufsichtsaufgaben wahr (vgl. Art. 81 ISG).

i. Fachstelle des Bundes für Informationssicherheit

Artikel 83 ISG schafft eine Fachstelle des Bundes für Informationssicherheit. Die ISV legt deren Aufgaben für den Zuständigkeitsbereich des Bundesrates fest. Die Fachstelle wird gestützt auf Artikel 85 ISG die nötigen organisatorischen, personellen, technischen und baulichen Vorgaben zur Gewährleistung der Informationssicherheit nach dem Stand der Technik beschliessen. Im internationalen Verhältnis wird sie die Rolle der nationalen Sicherheitsbehörde der Schweiz wahrnehmen (vgl. dazu Botschaft zum ISG, Ziff. 5.2 sowie Art. 41 Abs. 3 ISV).

3.4 Änderung der Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV)

Mit den Artikeln 24–26 ISG wurde die formell-gesetzliche Grundlage geschaffen, die für die Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen in den Identitätsverwaltungssystemen des Bundes nötig ist. Bei der vorliegenden Änderung der bestehenden IAMV werden vor allem formelle und technische Anpassungen vorgenommen. Neu wird allerdings der Geltungsbereich der IAMV auf die Verwaltungseinheiten der dezentralen Bundesverwaltung erweitert.

3.5 Verordnung über die Personensicherheitsprüfungen (VPSP)

a. Allgemeines

Mit der Verabschiedung des ISG hat der Gesetzgeber die Regelung über die PSP vom Bundesgesetz vom 21. März 1997[9] über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) ins ISG überführt. Gleichzeitig wurden die gesetzlichen Bestimmungen an die heutigen Bedürfnisse der Informationssicherheit angepasst. Für Prüfgründe ausserhalb der Informationssicherheit (z. B. Korruptionsbekämpfung) wurden Grundlagen in anderen Gesetzen geschaffen. Diese Modernisierung des Rechts der PSP soll auch dazu dienen, den Einsatz der Prüfungen auf das Mindestmass zu reduzieren, welches zur Identifizierung von erheblichen Risiken für den Bund erforderlich ist. Es wird eine Reduktion von mindestens 30% angestrebt, so dass die PSP mit den bestehenden Ressourcen innert nützlicher Frist bewältigt werden können. Die wichtigsten Änderungen am Rechtsrahmen der PSP sind im ISG selbst enthalten.

b. Gegenstand

Die neue Verordnung über die Personensicherheitsprüfungen (VPSP) fasst die Ausführungsbestimmungen zu den verschiedenen personenbezogenen Sicherheitsprüfungen in einem Erlass zusammen. Sie ersetzt die bisherige Verordnung vom 4. März 2011[10] über die Personensicherheitsprüfungen (PSPV), die bisherige Verordnung vom 9. Juni 2006[11] über die Personensicherheitsprüfungen im Bereich Kernanlagen (PSPVK) und alle bisherigen departementalen Verordnungen über die Personensicherheitsprüfungen[12].

Materiell regelt die Verordnung sowohl die PSP nach dem ISG als auch alle anderen Prüfungen, Beurteilungen und Kontrollen, die zwar nicht vom ISG vorgesehen sind, die aber nach dem Verfahren der PSP nach ISG durchgeführt werden. Ungeachtet ihrer Benennung oder des Prüfgrunds wird jedoch bei allen Prüfungen immer beurteilt, ob die betroffene Person für die Ausübung der massgebenden Tätigkeit vertrauenswürdig ist. Innerhalb derselben Prüfstufen werden dieselben Daten erhoben und dieselbe Beurteilungsmethode angewendet.

[9] SR **120**
[10] SR **120.4**
[11] SR **732.143.3**
[12] SR **120.421**–**120.427**

c. Straffung der Prüfgründe

Mit dem neuen Recht werden die Gründe zur Durchführung von PSP eingeschränkt. Funktionen, die der höchsten Prüfstufe, der erweiterten Personensicherheitsprüfung, zugeordnet werden, sollen die Ausnahme bleiben. Es besteht allerdings die Gefahr, dass der rechtliche Schwellenwert für die Prüfungen in der Praxis herabgesetzt wird, wenn die Ämter keine anderen Instrumente zur Verfügung haben, um die Vertrauenswürdigkeit ihrer Angestellten zu prüfen. Der neue Artikel 20*a* BPG bietet den Arbeitgebern hierzu entsprechende Mittel an.

d. Funktionenlisten

Um die Anzahl der Prüfungen im angestrebten Rahmen zu halten, bedarf es bei der Erstellung und Nachführung der Funktionenlisten, in denen die zu prüfenden Funktionen aufgelistet sind, einer besseren Kontrolle der Rechtmässigkeit der Einträge als heute. Das VBS soll deshalb die Funktionenlisten zentral bewirtschaften und sie auf Antrag der Departemente und die Bundeskanzlei (BK) laufend aktualisieren.

Die Listen der Funktionen, für die eine PSP nach dem ISG erforderlich ist, sind aus Sicht der Informationssicherheit sensitiv. Sie liefern den Überblick über sämtliche Funktionen von Verwaltung und Armee, die Zugang zu klassifizierten Informationen haben oder kritische Systeme des Bundes betreiben oder verwalten. Obwohl die Funktionenlisten keine Namen der Funktionsträgerinnen und -träger enthalten, ist es im Zeitalter der sozialen Medien für einen potenziellen Angreifer einfach, eine Funktion mit einem Namen zu verbinden und so ein Spionage- oder Sabotageziel zu erhalten. Im Bereich der Armee können zudem detaillierte Funktionenlisten Rückschlüsse auf die nicht veröffentlichte Detailorganisation der Armee ermöglichen. Die Funktionenlisten, welche die nach dem ISG zu prüfenden Funktionen beinhalten, sollen daher gestützt auf Artikel 6 des Publikationsgesetzes vom 18. Juni 2004[13] (PubIG) nicht veröffentlicht werden. Aus denselben Gründen werden die Funktionenlisten nach dem Stromversorgungsgesetz vom 23. März 2007[14] (StromVG) ebenfalls nicht veröffentlicht. Hingegen sollen die Listen der Funktionen, die in erster Linie zum Schutz vor Korruption oder vor Reputationsschaden einer Prüfung unterstellt werden, wie bis anhin veröffentlicht werden.

Die Funktionenlisten werden erst ab Eröffnung der Vernehmlassung des Ausführungsrechts zum ISG erstellt. Zuerst muss sichergestellt werden, dass die Prüfkriterien auf breite Akzeptanz stossen. Es handelt sich nämlich um mehrere Tausend potenzielle Einträge, die alle überprüft werden müssen, bevor sie in die definitiven Funktionenlisten aufgenommen werden. Detaillierte Angaben zum Aufwand für die PSP werden somit erst nach der Vernehmlassung vorliegen.

3.6 Verordnung über das Betriebssicherheitsverfahren (VBSV)

a. Allgemeines

Das ISG (vgl. Art. 49–72 ISG) führt das sogenannte Betriebssicherheitsverfahren ein. Das Verfahren befasst sich mit der Wahrung der Informationssicherheit bei der Vergabe von sicherheitsempfindlichen Aufträgen der Bundesbehörden an Betriebe, die nicht ihrer unmittelbaren Aufsicht unterstehen. Das Verfahren dient der Prüfung der Vertrauenswürdigkeit des zu beauftragenden Betriebs. Betriebe, die unter Einfluss von ausländischen Nachrichtendiensten stehen, sollen keinen Zugang zu sicherheitsempfindlichen Informationen oder zu kritischen Informatikmitteln des Bundes erhalten. Durch das neue Betriebssicherheitsverfahren wird die Risikomanagementmethode zur Reduktion nachrichtendienstlicher Ausspähung ausser Kraft gesetzt. Das Verfahren ermöglicht es zudem, die Umsetzung der Informationssicherheit während der Ausführung des Auftrags zu kontrollieren und durchzusetzen.

b. Gegenstand und Geltungsbereich

Die neue Verordnung über das Betriebssicherheitsverfahren regelt die Einzelheiten des Verfahrens und ersetzt die bisherige, auf militärisch klassifizierte Aufträge beschränkte Geheimschutzverordnung vom 29. August 1990[15]. Die VBSV gilt für sämtliche Behörden und Organisationen, die unter das ISG fallen. Für Verwaltungseinheiten der dezentralen Bundesverwaltung gilt die VBSV nur, wenn sie auch unter den Geltungsbereich der ISV fallen (vgl. Ziff. 3.3 Bst. b).

[13] SR **170.512**
[14] SR **734.7**
[15] SR **510.413**

c. Unterstellte Beschaffungen

In der Verordnung werden die Beschaffungen definiert, für welche das Verfahren in jedem Fall durchgeführt werden muss. Betroffen sind die Aufträge, bei denen GEHEIM klassifizierte Informationen zugänglich gemacht werden, sowie Beschaffungen von sensitiven Systemen, in denen VERTRAULICH klassifizierte Informationen mehrerer Organisationen bearbeitet oder die amts- und departementsübergreifend eingesetzt werden. Für alle anderen Beschaffungen wird die zuständige Fachstelle für Betriebssicherheit mit der auftraggebenden Stelle beurteilen, ob die Durchführung des Verfahrens angezeigt ist.

d. Abstimmung mit dem Beschaffungsrecht

Wie das ISG selbst weist die neue Verordnung zahlreiche Schnittstellen zur neuen Gesetzgebung des Bundes über das öffentliche Beschaffungswesen auf. Diese wurden bei der Erarbeitung des Vorentwurfs in Zusammenarbeit mit Vertretern der Fachämter detailliert geprüft und bereinigt. Die sachgerechte Durchführung des Betriebssicherheitsverfahrens setzt zudem eine enge Zusammenarbeit zwischen der auftraggebenden Stelle, der Beschaffungsstelle und der zuständigen Fachstelle für Betriebssicherheit voraus. Diese Zusammenarbeit soll zu einem möglichst frühen Zeitpunkt im Beschaffungsprozess stattfinden. Damit können beschaffungsbezogene Risiken früh identifiziert und reduziert werden.

3.7 Abstimmung von Aufgaben und Finanzen

Mit dem ISG und seinen Ausführungsverordnungen werden die Grundlagen für eine nachhaltige Verbesserung der Informationssicherheit der Bundesverwaltung und der Armee geschaffen. Dabei wird der Fokus auf die kritischsten Informationen und Informatikmittel gelegt. Die Einführung des ISMS ist dafür von zentraler Bedeutung: Es verbindet, steuert und überprüft alle Massnahmen und Prozesse des neuen Rechts. Ein effizientes Management der Informationssicherheit verbessert die Informationssicherheit effektiver, wirtschaftlicher und nachhaltiger als blosse Investitionen in technische Massnahmen.

Das Ambitionsniveau wurde sowohl für das ISMS als auch für die anderen Massnahmen ressourcenschonend festgelegt. Insgesamt werden deshalb die personellen und finanziellen Auswirkungen des ISG und seiner Verordnungen tief ausfallen. Es obliegt den Verwaltungseinheiten und den Departementen zu entscheiden, ob sie für ihren eigenen Zuständigkeitsbereich eine höhere Informationssicherheit haben und die entsprechenden Ressourcen zur Verfügung stellen wollen.

3.8 Umsetzung

Das Inkrafttreten des ISG und seiner Verordnungen ist auf Mitte 2023 geplant. Für einen erfolgreichen Übergang in das neue Recht sehen sowohl das ISG (vgl. Art. 90 ISG) als auch seine Ausführungsverordnungen (vgl. Art. 48 ISV, Art. 38 VPSP und Art. 25 VBSV) angemessene Übergangsfristen vor.

Vor dem Inkrafttreten des ISG und seiner Verordnungen müssen weitere Vorgaben erarbeitet oder aktualisiert werden, unter anderem:

- Vorgaben über das Management der Informationssicherheit im Bund (vgl. Art. 15 ISV);
- Klassifizierungskataloge (vgl. Art. 17 Abs. 2 und 3 ISV);
- Vorgaben über den Schutz von klassifizierten Informationen (vgl. Art. 21 Abs. 1 ISV);
- Vorgaben über die Sicherheitsakkreditierung von Informatikmitteln (vgl. Art. 23 Abs. 6 ISV);
- Vorgaben über die Mindestanforderungen für die jeweiligen Sicherheitsstufen der Informatiksicherheit (vgl. Art. 29 Abs. 1 ISV);
- Vorgaben über den physischen Schutz und die Sicherheitszonen (vgl. Art. 34 und 35 ISV);
- die Funktionenlisten für die Personensicherheitsprüfungen (vgl. Art. 3 VPSP).

Nebst dem Erlass von rechtlichen oder technischen Vorgaben müssen drei weitere Voraussetzungen erfüllt sein:

- Die Fachstelle des Bundes für Informationssicherheit (vgl. Art. 83 ISG) muss aufgebaut und in Betrieb genommen werden. Diese wird Aufgaben und Ressourcen aus dem heutigen Zuständigkeitsbereich des Generalsekretariats des VBS (Digitalisierung und Cybersicherheit VBS, DCS) und des Generalsekretariats des EFD (Nationales Zentrum für Cybersicherheit, NCSC) übernehmen. Der Bundesrat hat am 18. Mai 2022 beschlossen, das NCSC in ein Bundesamt zu überführen. Er hat das EFD beauftragt, bis Ende 2022 Vorschläge auszuarbeiten, wie das

Amt ausgestaltet und in welchem Departement es angesiedelt werden soll. Gleichzeitig werden diverse weitere Fragestellungen zu den sicherheitspolitischen Strukturen des Bundes, einschliesslich der Strukturen im Bereich Cyber, geklärt. Das Ergebnis dieser laufenden Arbeiten ist für die Ansiedlung der Fachstelle des Bundes für Informationssicherheit und ihre Ressourcen massgebend. Der Bundesrat wird erst nach der Vernehmlassung über die administrative Zuordnung der Fachstelle entscheiden.

- Die Informationssicherheitsbeauftragten und weitere Rollenträger müssen geschult werden.
- Mehrere Informationssysteme müssen angepasst oder eingeführt werden. Dies betrifft insbesondere SIBAD, das Informationssystem der PSP, und dessen Umsysteme sowie FABS, das künftige Informationssystem des Betriebssicherheitsverfahrens. Für einen effizienten Betrieb der ISMS durch die Ämter arbeitet der Bund an der Beschaffung und Einführung einer standardisierten ISMS-Anwendung, mit welcher die Aufgaben und Prozesse der Informationssicherheitsverordnung digitalisiert werden. Die ISMS-Anwendung soll Ende 2024 zur Einführung und Nutzung durch die Ämter und Departemente bereitstehen.

Die Umsetzungsarbeiten werden mit den anderen Bundesbehörden und mit den Kantonen koordiniert. Der Bundesrat wird bei Bedarf eine gestaffelte Inkraftsetzung des ISG und seiner Verordnungen beschliessen.

4 Erläuterungen zu einzelnen Artikeln

4.1 Informationssicherheitsverordnung (ISV)

Ingress

Der Ingress verweist auf sämtliche Gesetzesnormen, die dem Bundesrat eine Regelungskompetenz im Rahmen der ISV erteilen.

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Gegenstand

Der Begriff «Informationssicherheit» erfasst die Sicherheit aller Informationen, einschliesslich Personendaten nach der Gesetzgebung über den Datenschutz, für welche die Bundesverwaltung und die Armee verantwortlich sind. Die ISV regelt die Aufgaben, Verantwortlichkeiten und Kompetenzen sowie die Verfahren zur Gewährleistung der Informationssicherheit bei der Bundesverwaltung und bei der Armee, welche im Rahmen des Managements der Informationssicherheit, dem Schutz von klassifizierten Informationen, der Informatiksicherheit und der Massnahmen zur personellen und physischen Sicherheit erforderlich sind. Wie im ISG selbst (vgl. ISG-Botschaft, Erläuterungen zu Art. 1) wird der Begriff «Information» in der ISV nicht definiert. Wenn Personendaten im Sinne der Datenschutzgesetzgebung gemeint sind, wird jeweils der Begriff «Personendaten» verwendet.

Das Verhältnis zwischen dem ISG und dem Datenschutzgesetz vom 19. Juni 1992[16] (DSG) ist in der Botschaft zum ISG ausführlich erläutert (vgl. Botschaft ISG, Ziffer 1.2.3, S. 2977). Die Sicherheitsorgane nach den Artikeln 36 ff. ISV werden im Rahmen des ISMS die Koordination mit den zuständigen Datenschutzberaterinnen und Datenschutzberatern sicherstellen.

Art. 2 Geltungsbereich

Absätze 1–5: Im Rahmen einer Positivliste wird aufgeführt, für welche verpflichteten Behörden und Organisationen (vgl. ISG-Botschaft, Erläuterungen zur Artikel 2 ISG) und unter welchen Bedingungen diese Verordnung gilt.

Zur Geltung des ISG und der ISV für die Verwaltungseinheiten der dezentralen Bundesverwaltung nach Artikel 7*a* RVOV sowie für Organisationen nach Artikel 2 Absatz 4 RVOG, die mit Verwaltungsaufgaben betraut werden aber nicht der Bundesverwaltung angehören (vgl. Ziff. 3.3 Bst. b).

Für die verpflichteten Behörden nach Artikel 2 Absatz 1 Buchstabe a sowie c–e ISG (Bundesversammlung, eidgenössische Gerichte, Schweizerische Bundesanwaltschaft und ihre Aufsichtsbehörde sowie Schweizerischen Nationalbank) gilt diese Verordnung sinngemäss, sofern diese keine eigenen Ausführungsbestimmungen erlassen. Machen diese Behörden davon Gebrauch, sind sie von der ISV (nicht aber vom ISG) befreit.

[16] SR **235.1**

Absatz 6: Wenn die Kantone klassifizierte Informationen des Bundes bearbeiten, gelten die Bestimmungen des 4. Abschnitts dieser Verordnung. Wenn sie auf Informatikmittel des Bundes zugreifen, gelten für sie die Bestimmungen zur Zuordnung zu den Sicherheitsstufen (Art. 28), Sicherheitsmassnahmen (Art. 29), Sicherheit beim Betrieb (Art. 30) sowie physische Schutzmassnahmen (Art. 35). Die Kantone können sich allerdings von den bundesrechtlichen Vorgaben befreien, wenn sie von sich aus eine gleichwertige Informationssicherheit gewährleisten. Dies setzt voraus, dass sie eigene, an die Bundesstandards angeglichene Sicherheitsvorschriften erlassen, die sie in ihrem Zuständigkeitsbereich durchsetzen. Massgebende Bundestandards sind die Vorschriften und technischen Anforderungen für den Grundschutz der Informatik im Bund sowie für den Schutz von klassifizierten Informationen. Die Kantone sind nicht verpflichtet, ein ISMS nach Art. 5 ff. umzusetzen.

Eine «gleichwertige Informationssicherheit» liegt vor, wenn andere als in der ISV vorgesehene Sicherheitsvorkehrungen nach dem Stand der Technik gemäss Artikel 85 Absatz 1 ISG eine vergleichbare und mindestens gleich hohe beziehungsweise starke Wirkung erzielen. Die Kantone beurteilen in erster Linie in eigenem Ermessen, ob eine gleichwertige Informationssicherheit vorliegt.

Mit dem Begriff «Kantone» sind nebst den Kantonen gemäss Artikel 3 der Bundesverfassung[17] auch öffentlich-rechtliche Körperschaften, Anstalten oder Stiftungen erfasst, die dem Verwaltungsrecht des entsprechenden Kantons unterstehen. Es ist seitens Kantone in jedem Einzelfall zu prüfen, ob eine Organisation oder eine Anstalt (z. B. ein Spital, ein Elektrizitätswerk oder auch ein Finanzinstitut) als Kanton im Sinne des ISG beziehungsweise der ISV gilt. Fällt ein Kanton nicht unter den Geltungsbereich des ISG, wird er als Dritter im Sinne von Artikel 9 ISG behandelt (vgl. Erläuterungen zu Art. 10).

Absatz 6 Buchstabe b: Mit «Zugriff auf Informatikmittel» sind alle Arten von technischen Zugriffen seitens Kantone auf die Informatikmittel des Bundes gemeint. Die Zugriffsfrage muss in jedem Einzelfall geprüft werden. Ob ein Zugriff besteht, entscheidet letztlich der Bund.

2. Abschnitt: Grundsätze

Art. 3 Sicherheitsziele

Die Informatikmittel der Organisationen, die der ISV unterstellt sind, weisen zunehmend gemeinsame technische Schnittstellen auf. Aufgrund dessen können Risiken oder Bedrohungen der Organisation oder deren Lieferanten nicht isoliert betrachtet werden. Informationssicherheit ist zwangsläufig eine vernetzte Aufgabe, welche ein gemeinsames Ziel und ein koordiniertes Vorgehen verlangt.

Absatz 1: Der Bundesrat ist bestrebt, dass der Schutz von Informationen und Informatikmitteln nach einem risikobasierten Ansatz gewährleistet wird. Es genügt heute nicht mehr, Sicherheit lediglich nach einer Checkliste umzusetzen. Vielmehr müssen die Verantwortlichen ein aktives Risikomanagement betreiben, die Bedrohungen der Informationssicherheit und deren potenziellen Auswirkungen auf das Geschäft kennen, den Aufwand zum Minimieren von Risiken an deren Grösse anpassen beziehungsweise den Fokus auf die grössten Risiken legen und die effizientesten Massnahmen zur Risikominimierung einsetzen. Mit dem risikobasierten Ansatz soll der Fokus nicht nur auf die Risiken (negative Auswirkungen), sondern auch auf Möglichkeiten und Chancen (positive Auswirkungen) neuer Ideen, Anwendungen oder Technologien gelegt werden. Mit «Resilienz» ist die Widerstandsfähigkeit einer Organisation und die schnelle Wiederaufnahme des Normalbetriebs nach einem Sicherheitsvorfall gemeint.

Art. 4 Verantwortung

Absatz 1 und 2: Gemäss Artikel 45 RVOG die Direktorinnen und Direktoren der Gruppen und Ämter sind gegenüber ihren Vorgesetzten für die Führung der ihnen unterstellten Verwaltungseinheiten sowie für die Erfüllung der ihnen übertragenen Aufgaben verantwortlich. Dies schliesst die Verantwortung für die Informationssicherheit ein. Zwar legt das NCSC heute minimale Informationssicherheitsvorgaben fest, welche dem Schutz der gesamten Bundesverwaltung dienen und die Verwaltungseinheiten mit beschränktem Handlungsspielraum umsetzen müssen. Diese entbinden die Verwaltungseinheiten jedoch nicht von ihrer Verantwortung, die Risiken laufend zu beurteilen und, wenn nötig, weitergehende Massnahmen zu treffen. Zur Kompetenz der Departemente, gewisse Aufgaben anders zu verteilen, vgl. Erläuterungen zu Artikel 39 Absatz 3.

Absatz 3: Bei der Bearbeitung von Informationen oder bei der Nutzung der Informatikmittel des Bundes müssen die Mitarbeitenden die entsprechenden Verhaltensvorschriften einhalten. Die

[17] SR **101**

Wahrnehmung dieser Verantwortung setzt voraus, dass sie entsprechend instruiert und ausgebildet werden (vgl. Erläuterungen zu Art. 4 Abs. 4 und Art. 11 ISV).

Mit «Mitarbeitenden der Bundesverwaltung» sind interne und externe Mitarbeitende gemeint, die der Weisungsbefugnis des Bundes unterstehen: «Interne» Mitarbeitende sind Angestellte des Bundes gemäss BPG; «externe» Mitarbeitende hingegen sind Personen, die mittels eines Personalverleihvertrages angestellt sind. Keine Mitarbeitenden des Bundes sind hingegen selbständige Privatpersonen oder Mitarbeitende von Unternehmen, die beispielsweise basierend auf einem Vertragsverhältnis für den Bund beratend tätig sind oder für diesen Dienst- oder Sachleistungen erbringen (wie Softwareentwicklung, Netzwerkausbau, Bau eines Serverraums, Übernahme der Projektleitung etc.). Solche Personen gelten als «Dritte» (vgl. Erläuterungen zu Artikel 10). Bei Dritten ist die vorschriftsgemässe Handhabung hinsichtlich der Schutzobjekte ggf. über entsprechende Verträge im Sinne von Artikel 9 ISG sicherzustellen.

Absatz 4: Die Vorgesetzten aller Stufen tragen auch im Bereich der Informationssicherheit die Verantwortung für die funktionsbezogene, praxisnahe Instruktion und Ausbildung ihrer Mitarbeitenden sowie für die Überprüfung der Einhaltung der Vorschriften. Somit obliegt es den Vorgesetzten, ihren Mitarbeitenden praktisch zu erklären, wie sie mit geschützten Informationen umgehen müssen, sie auf den vorgabenkonformen konsequenten Einsatz von Verschlüsselungssoftware aufmerksam zu machen oder dafür zu sorgen, dass sie die angebotenen Schulungen besuchen. Zur Verantwortung der Verwaltungseinheiten, vgl. Erläuterungen zu Artikel 11.

3. Abschnitt: Management der Informationssicherheit

Die Artikel 5 bis 15 ISV definieren die minimalen Anforderungen an das Management der Informationssicherheit in der Bundesverwaltung und in der Armee. Sie legen für die Kernaufgaben der Informationssicherheit jeweils die Zuständigkeiten der Ämter, der Departemente und der Fachstelle des Bundes für Informationssicherheit fest. Letztere wird dazu Bearbeitungsvorgaben (vgl. Art. 21 Abs. 1) oder generell-abstrakte Weisungen (vgl. Art. 29 Abs. 1) erlassen, welche den risikobasierten Ansatz berücksichtigen.

Art. 5 Informationssicherheits-Managementsystem

Absatz 1: Ein ISMS umfasst Verfahren und Regeln, die aufzeigen, wie Informationssicherheit in einem System organisiert ist und macht sichtbar, welche Aufgaben, Kompetenzen und Verantwortlichkeiten entsprechenden Personen zugeordnet werden. Mit dem Begriff «ISMS» wird implizit auf die Norm ISO/IEC 27001 verwiesen, die sowohl in der Privatwirtschaft als auch vermehrt in öffentlichen Verwaltungen als Standard gilt. Von den Verwaltungseinheiten wird aber lediglich ein «ISMS light» verlangt; d.h. sie müssen nicht die ganze ISO-Norm umsetzen, sondern nur die wichtigsten in der ISV definierten Managementprozesse. Künftige Vorgaben werden diese Managementprozesse präzisieren. Eine externe Zertifizierung wird nicht verlangt. Den Verwaltungseinheiten und Departementen steht es jedoch frei, ein höheres Ambitionsniveau festzulegen.

Während die Sicherheitsverantwortlichen der Verwaltungseinheiten (vgl. Art. 36) den Aufbau, den Betrieb, die Überprüfung und die kontinuierliche Verbesserung des ISMS sicherstellen, obliegt der eigentliche Betrieb des ISMS dem Informationssicherheitsbeauftragten der Verwaltungseinheit (vgl. Art. 37 Abs. 2 Bst. a). Der Letztere wird vom Ersten beauftragt. Gemäss Artikel 48 Absatz 4 muss ein ISMS bis spätestens drei Jahre nach Inkrafttreten der ISV aufgebaut sein.

Absatz 2: Ein ISMS bezweckt, die Informationssicherheit in der Verwaltungseinheit zu führen und zu verbessern. Dafür werden konkrete Ziele benötigt, anhand derer die Amtsleitung beurteilen kann, ob es die gewünschte Wirkung erbringt. Diese jährliche Zielsetzung und -messung ist eine Führungsaufgabe der Amtsleitung und ist abzugrenzen von der Erstellung des jährlichen Kontroll- und Auditplans nach Artikel 13.

Absatz 3: Um eine gewisse Objektivität und Vergleichbarkeit bei der Bewertung der Umsetzung und Wirksamkeit des ISMS sicherzustellen, wird eine periodisch durchgeführte Überprüfung durch eine vom Amt unabhängige Stelle oder vom Departement verlangt. Diese unabhängige ISMS-Überprüfung schafft ein Vertrauen für die anderen Ämter und sorgt gleichzeitig für die kontinuierliche Verbesserung der Sicherheit im Amt selber.

Die Periodizität von drei Jahren richtet sich zwar nach dem offiziellen Zertifizierungszyklus der ISO-Norm, der Umfang der vorgeschriebenen Überprüfung ist jedoch deutlich weniger ambitiös als im ISO-Standard: Verlangt wird nicht zwangsläufig ein formelles Audit im Sinne der ISO-Norm, obschon ein solches Audit zu begrüssen wäre. Je nach Auftrag können zudem das gesamte

ISMS oder nur bestimmte Teile davon überprüft werden. Die betroffene Verwaltungseinheit trägt die Entscheidungsbefugnis über die Wahl einer unabhängigen Prüfstelle. Solche Prüfungen können entweder durch die internen Aufsichtsstrukturen der Departemente oder durch eine externe Firma durchgeführt werden (vgl. Aufführungen in ISG-Botschaft, S. 3018). Denkbar wäre auch der Einsatz eines Pools von ISMS-Auditoren aus den Verwaltungseinheiten eines Departements oder des Bundes. Der kontinuierliche Verbesserungsprozess ist für die Gewährleistung der Informationssicherheit zentral. Diesem wird mit solchen Überprüfungen Rechnung getragen.

Absatz 4: Absatz 4 zeigt den engen Bezug des ISMS zum Risikomanagement Bund, zum betrieblichen Kontinuitätsmanagement und zum Krisenmanagement auf. Es handelt sich dabei um Managementaufgaben, die ausserhalb des Geltungsbereichs der ISV liegen, welche aber die Verwaltungseinheiten eng aufeinander abstimmen und koordinieren müssen.

Art. 6 Pflege der Rechtsgrundlagen und vertraglichen Verpflichtungen

Absatz 1: Ein Verzeichnis über die im eigenen Zuständigkeitsbereich massgebenden Rechtsgrundlagen sowie vertraglichen Verpflichtungen im Bereich Informationssicherheit dient dem Nachweis der Einhaltung der relevanten Rechtsgrundlagen, welche es beispielsweise im Rahmen der Messung der jährlichen Zielerreichung des ISMS (vgl. Art. 5 Abs. 2 oder der ISMS-Überprüfung nach Art. 5 Abs. 3) zu prüfen gilt. Aufgrund der wachsenden Lieferketten im Bereich der Informationssicherheit ist eine Übersicht über die zu leistenden Verpflichtungen und zu beanspruchenden Rechte unabdingbar und fördert nicht zuletzt die Nutzung von Synergien anderer bereits bestehender Vertragsverhältnisse.

Absatz 2: Die Fachstelle des Bundes für Informationssicherheit ist zwingend beratend (Konsultationspflicht), sie hat jedoch keine inhaltliche Weisungsbefugnis. Beurteilungen und Einschätzungen einer Bundesfachstelle kommen jedoch ein grosses Gewicht zu. Abweichungen sollten stets gut begründet und insbesondere gleichwertig sein. Diese Konsultationspflicht bezieht sich auf sicherheitsrelevante Vorgaben (z. B. Weisungen und Richtlinien) oder Vorhaben (z. B. sicherheitsrelevante IT-Projekte) der Verwaltungseinheiten oder Departemente.

Art. 7 Inventarisierung der Schutzobjekte

Absatz 1: Ein Inventar enthält eine Auflistung sämtlicher Schutzobjekte gemäss Artikel 7 Absatz 2 zu einem bestimmten Zeitpunkt (sogenannte Inventarliste).

Absatz 2: Heute kennt die CyRV nur das «Informatikschutzobjekt» (vgl. Art. 3 Bst. h CyRV), was mit Buchstabe b abgedeckt wird. Informationen werden aber nicht immer in einem einzigen, dedizierten Informationssystem bearbeitet. Dies ist zum Beispiel der Fall, wenn eine Aufgabe in der allgemeinen Informatikumgebung des Bundes erfüllt wird oder die Informationen in einer externen Cloud bearbeitet werden. Mit dem Schutzobjekt «Informationen» im Sinne von Buchstabe a wird deshalb von der Abhängigkeit zu einem bestimmten Informatikmittel abgesehen und nur der Schutz der Informationen beurteilt, die zur Erfüllung der Aufgabe bearbeitet werden. Grundsätzlich kommen aber dieselben Kriterien und Methoden zur Beurteilung des Schutzbedarfs wie bei Informatikschutzobjekten zum Einsatz. Mit dem Begriff «Aufgabe des Bundes» wird nicht jede Aufgabe subsumiert, sondern wichtige Geschäftsprozesse einer Verwaltungseinheit. Die Vorgaben der Fachstelle des Bundes für Informationssicherheit (vgl. Art. 15) werden dies präzisieren.

Absatz 3: Nur eine aktuelle Inventarliste kann den laufenden Nachweis über alle die Schutzobjekte betreffenden Informationen nach den Buchstaben a–g gewährleisten.

Absatz 3 Buchstabe c: Die Möglichkeit der geteilten Nutzung der jeweiligen Schutzobjekte (vgl. Bst. e) verweist auf das «Once-Only-Prinzip». Dabei entscheiden die Verwaltungseinheiten in eigenem Ermessen, welche Schutzobjekte mit anderen Verwaltungseinheiten geteilt werden.

Absatz 3 Buchstabe d: Die Übersicht über vertragliche Bindungen zu Dritten (vgl. Erläuterungen zu Art. 10 Abs. 1 ISV), beispielsweise zu Informatiklieferanten, dient einerseits dem funktionierenden Lieferantenmanagement und ermöglicht es, eventuelle Abhängigkeiten des Bundes von Lieferanten frühzeitig zu erkennen (inkl. Beurteilung der Gefahr von Klumpenrisiken). Sie ermöglicht andererseits die Identifizierung von Risiken, die über diese Lieferanten Auswirkungen auf den Bund haben können.

Absatz 3 Buchstabe f: Bezüglich Restrisiken vgl. Erläuterungen zu Artikel 9.

Absatz 3 Buchstabe g: Vgl. Erläuterungen zu Artikel 14 in Verbindung mit 6 Absätze 2 und 3.

Art. 8 Risikomanagement

Absatz 1: Die Beurteilung der Risiken ist eine der Grundlagen für ein wirksames Risikomanagement und damit einer zweckmässigen und wirtschaftlichen Informationssicherheit (vgl. Aufführungen in ISG-Botschaft, S. 3018 f.). Die IT-Grundschutzvorgaben des Bundes bieten einen risikogerechten Schutz gegen eine Grosszahl von Bedrohungen. Sie dienen der vernetzten Informationssicherheit des Bundes und müssen eingehalten werden. Sie ermöglichen eine aufwandarme sicherheitsmässige Pflege von Informatikmitteln, die nicht besonders sicherheitsempfindlich sind. In diesem Fall müssen die Verwaltungseinheiten auch keine komplexen Risikobeurteilungen durchführen.

Es versteht sich von selbst, dass die Beurteilung der Risiken «nachweisbar» erfolgen muss. Die Nachweisbarkeit ist an keine bestimmte Form gebunden. Damit soll im Kontext der Digitalisierung der Einsatz technologieneutraler Nachweismethoden ermöglicht werden.

Absatz 1 Buchstabe a: Die Bewertung der Risiken hinsichtlich deren Auswirkung auf die Schutzobjekte (vgl. Art. 7 Abs. 2) ist in diesem Zusammenhang auch sehr technisch-operativ und richtet sich nach dem Bedarf an Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit der Informationen und des Informatiksystems.

Absatz 1 Buchstabe b: Die Kontrolle der Wirkung kann beispielsweise mittels Penetrationstests oder durch die Erhebung von relevanten Kennzahlen erfolgen.

Absatz 1 Buchstabe c: Vgl. Erläuterungen zum Vorgabemanagement nach Artikel 6.

Absatz 1 Buchstabe d: Verlangt wird ein bewusster Entscheid des Sicherheitsverantwortlichen, das heisst die nachweisbare Akzeptanz von Restrisiken auf Grundlage eines sorgfältig durchlaufenen Analyse- und Entscheidungsprozesses.

Absatz 3: Massgebend sind die Weisungen über die Risikopolitik des Bundes sowie die damit verbundenen Richtlinien und Handbücher.

Art. 9 Bewilligung und Verzeichnung von Ausnahmen

Mit Ausnahmemanagement ist die Bewirtschaftung der Ausnahmen der geltenden Informationssicherheitsvorgaben gemeint. Wie heute das NCSC wird mit der ISV die Fachstelle des Bundes für Informationssicherheit gestützt auf Artikel 85 ISG vorgeben, welche Mindestanforderungen im Bereich Sicherheit erfüllt werden müssen. Kann eine Verwaltungseinheit diese Mindestanforderungen nicht erfüllen, so kann sie eine Ausnahme beantragen. Die Fachstelle kann den Entscheid über Ausnahmen delegieren. So kann die Fachstelle des Bundes für Informationssicherheit selbst, das Departement oder eine bestimmte Person innerhalb des Amts über die Ausnahme entscheiden. Grundsätzlich kann das heutige Verfahren über die Ausnahmebewilligungen gemäss den aktuellen Bestimmungen der CyRV über die Subdelegation nach Absatz 2 übernommen werden.

Art. 10 Zusammenarbeit mit Dritten

Absatz 1: Als «Dritte» gelten gemäss ISG alle Behörden, Organisationen und Personen des öffentlichen oder privaten Rechts, die keine verpflichteten Behörden oder Organisationen sind und grundsätzlich unabhängig von diesen handeln. Auch dezentrale Verwaltungseinheiten gelten als Dritte, sofern sie nicht unter das ISG fallen (vgl. ISG-Botschaft S. 3013 und 3019 f.) oder gewisse Organisationen, die kritische Infrastrukturen betreiben (Art. 2 Abs. 5 ISG).

Absatz 3: Die Informationssicherheitsklauseln in den Verträgen haben die Voraussetzungen gemäss Artikel 9 ISG zu erfüllen (vgl. ISG-Botschaft zu Artikel 9).

Art. 11 Schulung und Sensibilisierung

Wenn die Bundesverwaltung und die Armee ihre Sicherheit nachhaltig verbessern wollen, müssen sie ihre Mitarbeitenden und Angehörigen so sensibilisieren und schulen, dass sie in der Lage sind, Gefahren und Bedrohungen selber zu erkennen, korrekt zu reagieren und entsprechende Sicherheitsmeldungen zu erstatten.

Die Verwaltungseinheiten stellen die generelle die Informationssicherheit betreffende Schulung (wie regelmässige Sensibilisierungs- und Awareness-Kampagnen oder Eintrittsschulungen) für sämtliche Mitarbeitende sowie das notwendige Budget, die Zeit und entsprechende Ressourcen sicher (vgl. Art. 4 Abs. 4). Dies im Gegensatz zu den direkten Vorgesetzten, die gemäss dieser Bestimmung für die funktionsbezogene Schulung ihrer Mitarbeitenden zuständig sind (vgl. Erläuterungen zu Art. 4 Abs. 4).

Art. 12 Vorfallmanagement

Absatz 1: Für die Bewältigung von Sicherheitsvorfällen und -lücken sind die Verwaltungseinheiten verantwortlich. Als «Sicherheitsvorfall» gilt ein Ereignis, bei dem die Informationssicherheit oder die entsprechenden Sicherheitsvorgaben verletzt werden oder wurden. Ein «Beinahe-Sicherheitsvorfall» gilt auch als Sicherheitsvorfall. Ein solcher liegt vor, wenn die Informationssicherheit hätte verletzt werden können. Als «Sicherheitslücke» gilt hingegen ein Mangel bei einem Informatikmittel, dessen Ausnutzung die Informationssicherheit verletzen kann. Wichtig ist die Festlegung vorab, wer im Ernstfall über Sofortmassnahmen entscheidet und wer bei solchen Entscheidungen zu konsultieren oder zu informieren ist. Wer die Entscheidkompetenz über Sofortmassnahmen inne hat, muss über das notwenige Verständnis der Auswirkung einer solchen Massnahme verfügen.

Absatz 2: Diese Bestimmung deckt sich zum heutigem Recht (vgl. Art. 14 Abs. Abs. 4 Bst. c CyRV), mit Ausnahme, dass neu auch «Beinahe-Sicherheitsvorfälle» zu melden sind.

Absätze 3 und 6: Mit der Kann-Vorschrift wird betont, dass die Fachstelle des Bundes für Informationssicherheit unterstützend tätig sein kann, aber eben nicht muss. Die Unterstützung der Fachstelle des Bundes für Informationssicherheit erfolgt grundsätzlich auf Anfrage der Verwaltungseinheiten oder Departemente und ist neben der Bedeutung und Wichtigkeit des Vorfalls auch abhängig von ihren Ressourcen (vgl. auch Absatz 6).

Absatz 4: Vgl. neue Meldepflichten für Verletzungen der Datensicherheit gemäss künftigem Datenschutzgesetz (nDSG, vgl. Art. 24), welches per 1. September 2023 in Kraft gesetzt werden soll.

Absatz 5 Buchstaben b und d: Vgl. ISG-Botschaft zu Artikel 17 beziehungsweise 88 ISG.

Absatz 5 Buchstabe e: Die hohe politische Bedeutung hängt von den betroffenen politischen Interessen ab. Diese ist in jedem Einzelfall zusammen mit der für die Sicherheit verantwortlichen Person des entsprechenden Departements (vgl. Art. 39) zu prüfen.

Absatz 7: Mit «Federführung» ist die operative Entscheidungskompetenz gemeint. Die Verantwortung für die Informationssicherheit trägt jedoch nach wie vor die Verwaltungseinheit oder das betroffene Departement (vgl. Erläuterungen zu Art. 4). Übernimmt die Fachstelle des Bundes für Informationssicherheit die Federführung, kann sie beispielsweise selbständig Sofortmassnahmen anordnen oder den Einsatz von Spezialisten (inkl. Dritte nach Art. 10) zur Unterstützung einsetzen. In diesem Zusammenhang anfallende Kosten gehen voll zu Lasten der verantwortlichen Verwaltungseinheit oder des Departements und erfolgen in Rücksprache mit diesen. Die Übernahme der Federführung hat nachweisbar zu erfolgen (vgl. Erläuterungen zu Art. 8 Abs. 1).

Art. 13 Planung von Kontrollen und Audits

Eine wesentliche Lücke im Management der Informationssicherheit der Bundesverwaltung und der Armee sind heute die fehlenden Kontrollen und Audits. Nur mit angemessenen Audits können Organisationen wissen, in welchem Zustand sich ihre Informationssicherheit befindet, welche Risiken bestehen und welche Korrekturmassnahmen erforderlich sind (vgl. ISG-Botschaft, S. 2978). Diese Bestimmung verlangt deshalb, dass die Verwaltungseinheiten und die Departemente jährlich festlegen, welche risikobasierten Kontrollen und Audits sie das nächste Jahr durchführen werden und wieso. Wird eine Überprüfung des ISMS nach Artikel 5 Absatz 3 ISV geplant, so ist diese Überprüfung in den Kontroll- und Auditplan einzutragen. Der Auditplan und die dafür nötigen Ressourcen werden durch die Sicherheitsverantwortliche oder den Sicherheitsverantwortlichen der Verwaltungseinheit genehmigt (vgl. Art. 36 Abs. 3 Bst. d). Artikel 13 legt nicht fest, wie viele Kontrollen und Audits durchgeführt werden müssen. Dieser Entscheid obliegt einzig der Verwaltungseinheit. Mit dem zwingend zu erstellenden Kontroll- und Auditplan muss die Amtsleitung einen positiven, nachvollziehbaren Entscheid treffen.

«Kontrollen» im Sinne dieser Verordnung sind punktuelle Überprüfungen, die einen eingeschränkten Geltungsbereich haben, informell mit wenigen Kräften durchgeführt werden können und oft günstiger sind als Audits. Zum Bespiel kann eine Verwaltungseinheit die Kontrolle der Aktualität der Sicherheitsdokumentation oder die Kontrolle der Einhaltung der «Clean-Desk»-Policy planen. «Audits» verlaufen hingegen nach einem formalisierten Verfahren und werden oft durch eine unabhängige Stelle durchgeführt. In einem Audit wird untersucht, ob Systeme, Prozesse oder Managementsysteme die geltenden Vorgaben oder geforderten Standards und Normen einhalten.

Absatz 2: Kontrollen und Audits können auch, sofern die Verträge mit Dritten dies zulassen, die Einhaltung der Vorschriften bei Dritten, beispielsweise bei Lieferanten, beinhalten. Wird eine solche Kontrolle geplant und verfügt der Dritte über eine Betriebssicherheitserklärung (vgl. Art. 61 ff.

ISG), soll eine Koordination mit der für das Betriebssicherheitsverfahren zuständigen Fachstelle Betriebssicherheit dazu dienen, dass der Bund nicht mehrmals dasselbe bei einem Partner kontrolliert.

Absatz 3: Die Fachstelle des Bundes für Informationssicherheit kann auf Antrag der Bundesbehörden Überprüfungen durchführen (vgl. Art. 83 Abs. 1 Bst. c ISG). Das Ambitionsniveau wird hier bewusst tiefgehalten und es wird zurzeit auf den Ausbau der Auditfähigkeit der Fachstelle des Bundes für Informationssicherheit verzichtet. Die Eidgenössische Finanzkontrolle (EFK) führt nämlich seit Jahren qualitativ hochwertige Audits und Querschnittsprüfungen im Bereich der Informationssicherheit durch. Diese Audits nehmen die Risiken, die im Fokus der Fachstelle des Bundes für Informationssicherheit stehen, ins Visier und decken damit den Bedarf auf Stufe Bund ab.

Art. 14 Berichterstattung

Absätze 1 und 2: Die Berichterstattung umfasst insbesondere: Den Stand und die Wirksamkeit der ISMS der Verwaltungseinheiten; den Stand der Schutzobjekte, der Umsetzung der Sicherheitsmassnahmen und der Übernahme der Restrisiken; den Stand der Ausbildung; Angaben über die für das Departement oder die BK durchgeführten Personensicherheitsprüfungen und Betriebssicherheitsverfahren; die Erkenntnisse aus Sicherheitsvorfällen und Sicherheitslücken sowie die getroffenen und geplanten Verbesserungsmassnahmen; die Erkenntnisse aus den Kontrollen und Audits sowie die getroffenen und geplanten Verbesserungsmassnahmen.

Absatz 3: Um eine nachhaltige Verbesserung der Informationssicherheit beim Bund bewirken zu können, ist eine kontinuierliche kritische Überprüfung der Wirksamkeit der Informationssicherheit sowie eine stete Anpassung sinnvoller Sicherheitsmassnahmen notwendig.

Art. 15 Vorgaben zum Management der Informationssicherheit

Dieser Artikel bezieht sich auf Artikel 85 ISG. Die Fachstelle hat vom Bundesrat die Kompetenz erhalten, die Vorgaben zum Management der Informationssicherheit (Art. 5–14) zu erlassen. Diese Vorgaben gelten nur für die Stellen nach Artikel 2 Absätze 1–3, welche im Zuständigkeitsbereich des Bundesrates liegen.

4. Abschnitt: Klassifizierte Informationen

Die Artikel 18–20 beschreiben die materiellen Voraussetzungen für die Klassifizierung von Informationen (vgl. ISG-Botschaft zu Art. 13). Im Vergleich zur heutigen ISchV wurden die Schwellenwerte für die Klassifizierung INTERN, VERTRAULICH und GEHEIM erhöht. Mit der Erhöhung der Schwelle für INTERN, VERTRAULICH und GEHEIM klassifizierte Informationen soll es künftig möglich sein, zielgerichteter zu klassifizieren. Damit sollte es in der Bundesverwaltung künftig insgesamt weniger klassifizierte Informationen geben, mit entsprechender Auswirkung auf die Ressourcen. Im Weiteren hat diese Massnahme einen direkten Einfluss auf die Anzahl Personensicherheitsprüfungen (PSP). Mit der Erhöhung der Klassifizierungsschwelle sollte es inskünftig weniger Funktionen geben, für deren Ausübung die Bearbeitung von VERTRAULICH klassifizierten Informationen erforderlich ist (vgl. VPSP sowie Erläuterungen dazu).

Art. 16 Grundsätze

Absatz 1: Die Klassifizierung ist zwingend, sofern die entsprechenden Kriterien nach den Artikeln 18 ff. ISV erfüllt sind. Das «Need-to-Know-Prinzip» nach Artikel 14 ISG ist strikt einzuhalten. Das Klassifizieren von Material ist ein Anwendungsfall der Klassifizierung von Informationen, für welchen grundsätzlich dieselben Beurteilungsmethoden und Schutzvorkehrungen gelten (inkl. Vorschriften gemäss VPSP und VBSV; vgl. ISG-Botschaft, S. 3020).

Absatz 2: Durch Zusammenfügung von klassifizierten oder nichtklassifizierten Informationen oder Informationsträgern (wie Papier, Hardware, Funkgeräte) kann ein Sammelwerk entstehen, welches einen höheren Schutzbedarf aufweist als eine darin enthaltene isolierte Information. Dies ist typischerweise bei Datenbanken der Fall (z. B. das Produkt «deepl.com» als Cloud-Lösung oder beim Hosting des Intranets Bund, da das Hosting in der Cloud stattfinden kann). Ebenfalls können inskünftig vermehrt durch künstliche Intelligenz getriebene Produkte aus simplen isolierten Informationen zu klassifizierende Sammelwerke entstehen.

Absatz 3: Ob ein Dokument basierend auf dem Öffentlichkeitsprinzip beispielsweise einer Journalistin ausgehändigt wird, hängt nicht von seinem allfälligen Klassifizierungsvermerk ab, sondern bestimmt sich einzig nach den Kriterien des Öffentlichkeitsgesetzes vom 17. Dezember 2004[18] (BGÖ).

Art. 17 Klassifizierende Stellen

Absatz 1: Klassifizierende Stellen nach dieser Verordnung sind sämtliche Mitarbeitende des Bundes (vgl. Art. 4 Abs. 3) und Angehörige der Armee. Dritte sind keine klassifizierenden Stellen. Die in Buchstaben a, b und c genannten Personen sind für die Klassifizierung und auch für die Entklassifizierung zuständig. Spezialfälle sind zu berücksichtigen, so im Rahmen von Projektgeschäften: Nach HERMES ist zum Beispiel der Auftraggeberin des Projekts (und nicht die Projektleiterin oder der Projektleiter) dafür verantwortlich, dass allfällig entstehende Informationssammlungen hinsichtlich eines zu klassifizierenden Sammelwerks überprüft werden.

Allgemein gilt es sicherzustellen, dass die schutzwürdige Information genau ab dem Zeitpunkt, da sie optisch und/oder akustisch wahrnehmbar ist, geschützt (z. B. klassifiziert) wird. Wenn das nicht unmittelbar an der Quelle passiert, ist es meistens schon zu spät. Linienvorgesetzte oder die Auftraggeberin der klassifizierenden Stellen dürfen die Klassifizierung anpassen. Sie müssen bei einer solchen Übersteuerung, welche eine Verantwortungsübernahme hinsichtlich der Richtigkeit der Klassifizierung beinhaltet, aber eindeutig als die klassifizierende Stelle in Erscheinung treten. Ist die klassifizierende Stelle nicht mehr eruierbar, besteht die Möglichkeit, die Nachfolgeorganisation über das Schweizerische Bundesarchiv (BAR) ausfindig zu machen.

Absatz 2: Die heutigen Weisungen über die Klassifizierung (Klassifizierungskatalog) vom 26. September 2011 (vgl. Art. 8 ISchV) werden bis vor Inkrafttreten des ISG überarbeitet.

Absatz 4: Diese Bestimmung entspricht dem heutigen Artikel 8 ISchV, wobei die Kompetenz von der Generalsekretärenkonferenz zur Fachstelle des Bundes für Informationssicherheit übertragen wird.

Art. 18 Klassifizierungsstufe «intern»

Damit eine Klassifizierung als INTERN gerechtfertigt ist, sind zwei Voraussetzungen kumulativ erforderlich: So muss die Kenntnisnahme von Informationen durch Unberechtigte zu einer kausalen *potenziellen* Beeinträchtigung der öffentlichen Interessen der Schweiz führen können beziehungsweise die Beeinträchtigung darf nicht einfach vernachlässigbar sein, ohne dass konkrete Angaben für einen finanziellen Schaden vorgegeben werden sollen; gemäss ISchV ist lediglich ein nicht näher umschriebener «Nachteil» verlangt. Diese öffentlichen Interessen werden in Artikel 1 Absatz 2 Buchstaben a–d ISG wiedergegeben; der Buchstabe e ist eben gerade kein eigenes Schutzinteresse der Bundesinstitution (vgl. ISG-Botschaft, S. 3022 f.). Solche Informationen werden per Gesetz oder Vereinbarung geschützt; ebenfalls sorgen das Amtsgeheimnis nach Artikel 321 des Strafgesetzbuchs vom 21. Dezember 1937[19] oder das BGÖ in den in diesen Gesetzen vorgesehenen Fällen für den Schutz bestimmter Informationen.

Artikel 19 Klassifizierungsstufe «vertraulich»

Damit eine Klassifizierung als VERTRAULICH gerechtfertigt ist, sind zwei Voraussetzungen kumulativ erforderlich: So muss die Kenntnisnahme von Informationen durch Unberechtigte zu einer kausalen und potenziell *erheblichen* Beeinträchtigung der öffentlichen Interessen der Schweiz führen können. Diese Interessen werden in Artikel 1 Absatz 2 Buchstaben a–d ISG wiedergegen. Mit «erheblich» ist gemeint, dass der Schweiz oder dem Bund ein gewichtiger Schaden entstehen könnte.

Artikel 20 Klassifizierungsstufe «geheim»

Damit eine Klassifizierung als GEHEIM gerechtfertigt ist, sind zwei Voraussetzungen kumulativ erforderlich: So muss die Kenntnisnahme von Informationen durch Unberechtigte zu einer kausalen und potenziell *schwerwiegenden* Beeinträchtigung der öffentlichen Interessen des Bundes führen können. Diese Interessen werden in Artikel 1 Absatz 2 Buchstaben a–d ISG wiedergegeben. Mit «schwerwiegend» ist gemeint, dass der Schweiz ein katastrophaler Schaden entstehen könnte.

[18] SR **152.3**
[19] SR **311.0**

Art. 21 Bearbeitungsvorgaben

Absatz 1: Gestützt auf Artikel 85 ISG erlässt die Fachstelle des Bundes für Informationssicherheit Vorgaben über die Bearbeitung von klassifizierten Informationen und die organisatorischen, personellen, technischen und baulichen Anforderungen für deren Schutz. Diese Vorgaben gelten nur für die Stellen nach Artikel 2 Absätze 1–3.

Absatz 4: In Anwendung von Artikel 84 Absatz 1 ISG überträgt der Bundesrat die Kompetenz zur Regelung der Bearbeitung klassifizierter Bundesratsgeschäfte an die BK.

Absatz 5: Völkerrechtliche Verträge im Bereich der Informationssicherheit enthalten beispielsweise Konkordanzlisten über die Anwendung von Klassifizierungen, Sicherheitsstandards im Bereich der Informatik oder Kommunikationssicherheit sowie Regelungen über die Durchführung gegenseitiger Kontrollen (vgl. ISG-Botschaft zu Art. 88).

Art. 22 Einsatzbezogene Sicherheitsmassnahmen

Es kann vorkommen, dass der Bedarf, Informationen rasch zu teilen, höher als der Schutz der Vertraulichkeit zu bewerten ist. Dies ist insbesondere bei Einsätzen von Sicherheits- oder Polizeikräften der Fall. In diesen Fällen kann eine zielgerichtete Vereinfachung der normalen Sicherheitsvorschriften die Aufgabenerfüllung verbessern, ohne ein untragbares Risiko einzugehen. Gemäss heutigem Recht (vgl. Art. 18 Abs. 3 ISchV) können die Nachrichtendienste und fedpol klassifizierte Informationen vereinfacht handhaben. Derselbe Bedarf haben weitere mit Sicherheitsaufgaben betrauten Verwaltungseinheiten des Bundes, insbesondere die Gruppe Verteidigung, weshalb die vereinfachte Bearbeitung weiteren Stellen zugänglich gemacht werden soll. Allerdings darf diese Möglichkeit nicht zum absurden Ergebnis führen, dass für die sicherheitskritischsten Ämter *generell* tiefere Sicherheitsanforderungen gelten als für die anderen Ämter. Deshalb werden die Bedingungen und Modalitäten der vereinfachten Bearbeitung im Vergleich zu heute leicht verschärft.

Art. 23 Sicherheitsakkreditierung von Informatikmitteln

Absatz 1: Neu führt die ISV für eine begrenzte Anzahl sicherheitsempfindlicher Informationssysteme (vgl. Bst. a–c), in denen VERTRAULICH oder GEHEIM klassifizierte Informationen mehrerer Organisationen bearbeitet werden (beispielsweise eine Anwendung für die vertrauliche Videokommunikation), eine Akkreditierungspflicht ein. Bevor eine Sicherheitsakkreditierung erteilt wird, darf das entsprechende Informatikmittel nicht eingesetzt werden. Die Sicherheitsakkreditierung wird im Ausland und im internationalen Verhältnis immer dann verlangt, wenn geschützte Informationen einer Behörde (oder eines Staates) in einem System einer anderen Behörde (oder eines anderen Staates) bearbeitet werden sollen. Die ISV schliesst damit eine Lücke, welche die internationale Zusammenarbeit im Sicherheitsbereich bisher erschwert hat.

Absätze 2-4: Die Sicherheitsakkreditierung soll Vertrauen dafür schaffen, dass ein Informatikmittel die Anforderungen der Informationssicherheit des Bundes erfüllt. Kann die Sicherheitsakkreditierung nicht erteilt werden, entscheidet der Bundesrat über die Tragung der Restrisiken.

Absätze 5 und 6: Der richtige Umfang für die Akkreditierung wird im konkreten Einzelfall immer zu definieren sein. Diese Aufgabe wird der Fachstelle des Bundes für Informationssicherheit als künftige Akkreditierungsstelle zugeteilt; eine entsprechende Subdelegation im Bereich militärischer Systeme ist in Buchstabe c vorgesehen.

Art. 24 Schutz bei der Gefährdung von klassifizierten Informationen

Das ist bereits heute geltendes Recht (vgl. Art. 15 ISchV). Die Meldung an die zuständigen Sicherheitsorgane erfolgt nach der Bestimmung für das Vorfallmanagement (Art. 12).

Art. 25 Überprüfung von Schutzbedarf und Kreis der Berechtigten

Das ist bereits geltendes Recht (vgl. Art. 14 ISchV).

Art. 26 Archivierung

Absatz 1: Die Archivierungsbestimmungen regeln die Sicherung archivwürdiger Unterlagen des Bundes (einschliesslich klassifizierter Unterlagen) und deren Vermittlung an die Öffentlichkeit unter Berücksichtigung berechtigter Interessen des Persönlichkeits- und des Staatsschutzes sowie der Transparenz und der Nachvollziehbarkeit.

Absatz 2: Das BAR hat die Aufgabe, den Schutz des vom zentral archivierten und klassifizierten Archivguts zu gewährleisten. Es kann somit von den Standardanforderungen und –massnahmen der Fachstelle des Bundes für Informationssicherheit nach Artikel 85 ISG abweichen. Das BAR muss klassifiziertes Archivgut jedoch so schützen, dass die umgesetzte Sicherheit dem vom Archivgut ausgehenden Risiko entspricht.

Absatz 3: Die Schutzfrist von Archivgut (inkl. klassifiziertem Archivgut) wird nach deren Ablauf nicht automatisch verlängert. Die Klassifizierung hingegen entfällt automatisch mit Ablauf der Schutzfrist. Das heisst, nach Ablauf der Schutzfrist besteht ein umfassendes Einsichtsrecht in das Archivgut (vgl. Art. 10 Abs. 1 der Archivierungsverordnung vom 8. September 1999[20] (VBGA)). Die meisten klassifizierten Informationen erfordern nach Ablauf der 30- oder 50-jährigen Schutzfrist keine Verlängerung derselben. Hingegen kann es beispielsweise bei bestimmten militärischen Bauten oder Projekten gerechtfertigt sein, die Schutzfrist vor deren Ablauf zu verlängern (vgl. Art. 12 des Archivierungsgesetzes vom 26. Juni 1998[21] (BGA) in Verbindung mit Art. 14 VBGA).

Für die rechtzeitige Initiierung einer Verlängerung der Schutzfrist ist das zuständige Amt verantwortlich. Die Schutzfristen für die abgelieferten Unterlagen sind dem Ablieferungsverzeichnis zu entnehmen, welches die zuständige Verwaltungseinheit in den GEVER-Systemen (ActaNova) verwaltet. Bestände, die aufgrund überwiegender schutzwürdiger öffentlicher und privater Interessen verlängert geschützt werden (vgl. Art. 12 BGA und Art. 14 VBGA), werden im Anhang 3 der VBGA aufgeführt (vgl. Art. 14 Abs. 5 VBGA).

5. Abschnitt: Sicherheit beim Einsatz von Informatikmitteln

Art. 27 Sicherheitsverfahren

Das heutige Sicherheitsverfahren gemäss Artikel 14*b*–14*e* CyRV wird grundsätzlich übernommen.

Absatz 1: Der aktuelle Schutzbedarf ist mittels den Kriterien der Sicherheitsstufen gemäss Artikel 28 zu erheben.

Absatz 2: Abweichungen zu den Vorgaben erfordern stets eine ausdrückliche Bewilligung der Vorgabestelle (vgl. Erläuterungen zur Bewilligung von Ausnahmen nach Art. 9 ISV).

Der heute bei den Informatikvorgaben verankerte Risikomanagementmethode zur Reduktion nachrichtendienstlicher Ausspähung wird durch die Regelungen zum Betriebssicherheitsverfahren abgedeckt und benötigt keine gesonderte Regelung mehr (vgl. Art. 55–58 ISG).

Absatz 3: Ein Restrisiko kann grundsätzlich ein akzeptiertes Risiko oder unbekanntes Risiko sein (vgl. Handbuch Risikomanagement Bund). Ein Restrisiko nach der ISV ist einzig das Erstere. Wenn das ursprüngliche Risiko mittels Risikosteuerungsmassnahmen (wie Risikovermeidung, Risikoverminderung oder Risikotransfer) auf ein angemessenes Mass reduziert wird, spricht man vom Restrisiko.

Absatz 4: Die «nachweisbare» (vgl. Erläuterungen zu Art. 8 Abs. 2) Akzeptanz von Restrisiken ist wichtig, denn diese bestätigt einen durchlaufenen Analyse- und Entscheidungsprozess und damit einen bewussten Entscheid über die in Kauf genommenen Restrisiken. Die Delegation dieses bewussten Entscheids kann generell über eine Weisung oder fallweise (z. B. im Rahmen eines IT-Projekts) an ein anderes Geschäftsleitungsmitglied (ebenfalls nachweisbar) erfolgen.

Absätze 5 und 6: Mit einer neuen oder wiederkehrenden Bedrohung kann eine bereits vorliegende Risikoanalyse ganz oder teilweise in Frage gestellt werden, weshalb das Risikokonzept gegebenenfalls anzupassen ist.

Aufgrund der rasant fortschreitenden Technologieentwicklung und stets zunehmend komplexeren Bedrohungslagen im Informationssicherheitsbereich muss jährlich überprüft werden, ob eine sicherheitsrelevante Änderung stattgefunden hat. Damit entfällt auch die fünfjährige Frist zur Wiederholung des Sicherheitsverfahrens gemäss Artikel 14*e* Absatz 1 CyRV.

Art. 28 Zuordnung zu den Sicherheitsstufen «hoher Schutz» und «sehr hoher Schutz»

Neu werden Informatikmittel (vgl. Legaldefinition Art. 5 Bst. a in Verbindung mit Art. 17 ISG) in drei Sicherheitsstufen unterteilt: «Grundschutz», «hoher Schutz» und «sehr hoher Schutz». Dies im Unterschied zur heutigen CyRV, die nur zwei Sicherheitsstufen vorsieht: «Grundschutz» und «erhöhter

[20] SR **152.11**
[21] SR **152.1**

Schutz». Massgebend für die Einordnung in eine der drei neuen Schutzstufen sind die öffentlichen Interessen des Bundes nach Artikel 1 Absatz 2 Buchstaben a–e ISG. Der «Grundschutz» gilt neu auch für die Kantone (vgl. Art. 3 ISG), sofern diese unter den Anwendungsbereich des ISG fallen.

Im Gegensatz zu den Einstufungskriterien für klassifizierte Informationen wird im Rahmen der Sicherheitseinstufung der Informatikmittel auf finanzielle Kriterien abgestellt. Dies deshalb, weil eine Verletzung der Verfügbarkeit oder Integrität von Informationen, die mit Informatikmitteln bearbeitet werden, besser quantifizierbar ist als beispielsweise eine Verletzung der Vertraulichkeit eines klassifizierten Dokuments. Die finanziellen Kriterien richten sich nach den Kriterien der Bewertungsmatrix aus dem Risikomanagement Bund.

Art. 29 Sicherheitsmassnahmen

Absatz 1: Die Fachstelle des Bundes für Informationssicherheit erlässt gestützt auf Artikel 85 ISG Vorgaben über die Mindestanforderungen für die jeweiligen Sicherheitsstufen nach Artikel 17 ISG. Diese gelten nur für die Stellen nach Artikel 2 Absätze 1–3.

Absatz 2: Die Fachstelle des Bundes für Informationssicherheit sorgt betreffend Fragen rund um den Datenschutz und der risikobasierten Datensicherheit für eine sinnvolle Koordination mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten des Bundes (EDÖB) und den Datenschutzberatern gemäss DSG (vgl. auch Art. 82 Abs. 1 ISG). Zum risikobasierten Ansatz, vgl. Erläuterungen zu Artikel 4 Absatz 1. Die Weisungen der Fachstelle gemäss Absatz 1 sind mit den geltenden Datenschutzbestimmungen abzustimmen. In diesem Zusammenhang ist zu beachten, dass die Begriffe «hoher Schutz» und «sehr hoher Schutz» nach Artikel 17 ISG beispielsweise nicht mit den datenschutzrechtlichen Begriffen «Risiko» «geringes Risiko» oder «hohes Risiko» übereinstimmen.

Absatz 3: Mit den Buchstaben a und b wird zwischen zwei Arten von Risiken unterschieden, welche eine besondere Aufmerksamkeit hinsichtlich der Wirksamkeit der Sicherheitsmassnahmen fordern. Aus diesem Grund ist eine entsprechende Überprüfung fällig, sobald sich wesentliche Änderungen der Risiken abzeichnen, spätestens aber alle fünf Jahre. Die Rechtgrundlage für die periodische Überprüfung findet sich in Artikel 18 Absatz 3 ISG.

Absatz 4: Vgl. Erläuterungen zu Artikel 5 Absatz 4.

Art. 30 Sicherheit beim Betrieb

Absatz 1–4: Die internen Leistungserbringer des Bundes haben bei der Umsetzung der Informationssicherheit eine doppelte Rolle. Einerseits sind sie normale Verwaltungseinheiten, welche die ISV wie alle anderen Verwaltungseinheiten umsetzen müssen. Andererseits sind sie auch für die Sicherheit der Leistungsbezüger von zentraler Bedeutung. Es ist für die Sicherheit deshalb entscheidend, dass die Aufgaben- und Kompetenzteilung klar ist. Die Leistungserbringer haben eine allgemeine Pflicht, ihre Informatikleistungen nach dem Stand der Technik zu erbringen und ihren Leistungsbezügern die nötigen sicherheitsrelevanten Informationen zeitgerecht zur Verfügung zu stellen. Die Verwaltungseinheiten (in der Regel als Leistungsbezüger) sind allerdings dafür verantwortlich, dass die Verantwortlichkeiten für die Sicherheit auf betrieblicher Ebene, einschliesslich für das Schwachstellenmanagement, in den Leistungsvereinbarungen klar festgelegt werden. Sie sind nämlich für die Sicherheit ihrer Daten und Aufgaben verantwortlich.

Absatz 5: Diese Überwachung ist eine reine sicherheitstechnische Angelegenheit, die nichts mit einer allfälligen Überwachung der Mitarbeitenden zu tun hat. Dritte können beispielsweise Personen im Rahmen eines Bug-Bounty-Programms sein.

6. Abschnitt: Personelle Massnahmen und physischer Schutz

Art. 31 Prüfung der Identität von Personen und Maschinen

Absatz 1: Gestützt auf Artikel 85 ISG erlässt die Fachstelle des Bundes für Informationssicherheit nach Konsultation der oder des DTI-Delegierten Weisungen über minimalen technischen Anforderungen an die risikobasierte Prüfung der Identität von Personen und Maschinen, die Zugang zu Informationen, Informatikmitteln, Räumlichkeiten und anderen Infrastrukturen des Bundes benötigen. Diese Vorgaben gelten nur für die Stellen nach Artikel 2 Absätze 1–3.

Es geht hier darum festzulegen, wie gut eine Person ihre physische oder elektronische Identität nachweisen muss, um Zugang zu Informationen, Informatikmitteln, Räumlichkeiten und anderen Infrastrukturen des Bundes zu erhalten. Das erforderliche Sicherheitsniveau (das sogenannte

«level of assurance») wird bei sicherheitsempfindlichen Systemen höher als bei normalen Anwendungen sein. Nicht nur Personen, sondern auch Computer und sogar Prozesse müssen sich entsprechend «ausweisen».

Art. 32 Personensicherheit

Absatz 1: Die Verwaltungseinheiten müssen jährlich die Sensibilisierung der Mitarbeitenden sicherstellen, die einer PSP unterliegen. Die Vorgesetzten müssen ihre Verantwortung für die personenbezogenen Sicherheitsrisiken aktiv wahrnehmen und sie in die ständigen Führungsaufgaben integrieren. Beispielsweise könnte eine solche Sensibilisierung im Rahmen des Mitarbeitergesprächs erfolgen. Damit würde dieser Punkt mindestens einmal pro Jahr angesprochen.

Absatz 2: Die Praxis hat gezeigt, dass personenbezogene Sicherheitsrisiken nach bestandener PSP nur in Ausnahmefällen wieder thematisiert werden. Im Sinne einer international üblichen Nachsorge (sogenanntes «aftercare») sollen sicherheitsgeprüfte Mitarbeitende ihrem Arbeitgeber Umstände aus ihren privaten und beruflichen Umfeld, welche die Sicherheit gefährden, melden müssen. Solche Umstände können Vorfälle sein, die eine realistische Erpressbarkeit eines oder einer Mitarbeitenden hervorrufen (z. B. Grosse Verschuldung im Rahmen einer Spielsucht, aufgedeckte Alkohol- oder Drogensucht durch eine dritte Person, aufgeflogene ausserehe liche Beziehung). Falls eine Meldung erfolgt, wird das Vorgehen in Zusammenarbeit mit dem Personaldienst abgestimmt.

Art. 33 Verdacht auf strafbares Verhalten

Absatz 1: Die Bestimmung soll sicherstellen, dass mögliche Straftaten so schnell wie möglich den zuständigen Strafverfolgungsbehörden überwiesen werden, ohne dass sich die Departemente ausführliche Überlegungen strafrechtlicher oder gar strafprozessualer Natur machen müssen. In diesem Sinne kommt eine strafbare Handlung bereits «in Betracht», wenn erste, auch nicht vollends schlüssige Anzeichen auf strafbares Verhalten hindeuten.

Absatz 2: Hier geht es um die rasche Sicherung greifbarer und teils flüchtiger Beweise. Dafür dürfen keine allzu hohen Hürden aufgestellt werden. Wichtig ist, dass die Verwaltungseinheiten im Rahmen ihrer Beweissicherung keine physischen oder elektronischen Spuren verwischen, hinterlassen oder gar legen. Das hier gemeinte Sichern von Beweisen meint somit nicht auch deren Auswertung; dies ist gegebenenfalls Sache der Strafverfolgungsbehörden auf richterliche Anordnung.

Art. 34 Physische Schutzmassnahmen

Absatz 1: Gestützt auf Artikel 85 ISG erlässt die Fachstelle des Bundes für Informationssicherheit nach Konsultation der für die Objektsicherheit zuständigen Stellen der Bundesverwaltung und der Armee über die minimal erforderlichen Massnahmen zum physischen Schutz von Informationen und Informatikmitteln. Diese Vorgaben gelten nur für die Stellen nach Artikel 2 Absätze 1–3.

Absätze 1 und 2: Als physische Schutzmassnahmen gelten beispielsweise Errichtung von Sicherheitszonen (vgl. Art. 35 und ISG-Botschaft, S. 3032 ff.), Eingangskontrollen in Gebäude, Kameraüberwachungen gewisser Bereiche, Vorrichtungen zur Vernichtung von Informationsträgern oder Arbeitsplatzkontrollen. Für die Durchführung letzterer ist neu die oder der Informationssicherheitsbeauftragte der Verwaltungseinheiten (vgl. Art. 37 Abs. 2 Bst. j) zuständig.

Art. 35 Sicherheitszonen

Absatz 1: Durch die Schaffung von Sicherheitszonen soll das Schadenpotenzial infolge Spionage oder Sabotage in hochsensiblen Zonen (wie Server- oder Führungsräumen) reduziert werden (vgl. ISG-Botschaft S. 3015, 3032 ff.).

Absatz 2: Mit der Bestätigung der Sicherheitsanforderung für die Sicherheitszonen ist keine Sicherheitsakkreditierung nach Artikel 23 gemeint. Sicherheitszonen sind auch nicht mit abhörsicheren Räumen zu verwechseln, für die weiterreichende bauliche und organisatorische Massnahmen nötig sind.

Absatz 3: Gestützt auf Artikel 85 ISG erlässt die Fachstelle des Bundes für Informationssicherheit nach Konsultation der für die Objektsicherheit zuständigen Stellen der Bundesverwaltung und der Armee Vorgaben über die Sicherheitsanforderungen für die Sicherheitszonen und deren Einrichtung. Diese Vorgaben gelten nur für die Stellen nach Artikel 2 Absätze 1–3.

7. Abschnitt: Sicherheitsorganisation

Eine wichtige Neuerung in der ISV betrifft die Amtsleitungen. Ihnen werden in der ISV konkrete Aufgaben, Kompetenzen und Verantwortlichkeiten im Bereich Informationssicherheit übertragen, die sie bei Bedarf einem Mitglied ihrer Geschäftsleitung delegieren dürfen (Sicherheitsverantwortliche). Die Sicherheitsverantwortlichen werden das ISMS des Amts beaufsichtigen und alle wichtigen Entscheide im Bereich Informationssicherheit treffen. Die operativen Aufsichtstätigkeiten sind Aufgabe der Informationssicherheitsbeauftragten. Mit der ISV werden die heutigen Rollen der «Informatiksicherheitsbeauftragten» und der «Informationsschutzbeauftragten» in der neuen Rolle der «Informationssicherheitsbeauftragten» vereint. Ihre Aufgaben werden entsprechend präzisiert und mit ISMS-relevanten Aufgaben ergänzt.

Ein analoges Modell gilt auf Stufe der Departemente. Die Departemente sind im Sinne der Artikel 37, 38, 41 und 42 RVOG für die Steuerung, Koordination und Überwachung der Informationssicherheit im Departement verantwortlich. Sie bestimmen insbesondere die Informationssicherheitspolitik und die Sicherheitsorganisation des Departements. Die operative Verantwortung für die Sicherheit soll von der Generalsekretärin oder dem Generalsekretär getragen werden. Die Informationssicherheitsbeauftragten nehmen wie bis anhin die operativen Koordinations- und Aufsichtsaufgaben wahr (vgl. Art. 81 ISG).

Die Sicherheitsorganisation unter dem 7. Abschnitt beschreibt die verschiedenen vorgesehen Rollen und Funktionen. Gewisse Rollen wie diejenige der Informationssicherheitsbeauftragten der Verwaltungseinheiten (vgl. Art. 37) können je nach Bedürfnissen eines Amts von mehreren Personen themenspezifisch besetzt werden. Das gleiche gilt für alle anderen Rollen nach den Artikeln 37 ff. Keine Rolle ist nur an eine Person gebunden. Davon ausgenommen ist die Rolle nach Artikel 35: Der Sicherheitsverantwortliche der BK und der Verwaltungseinheiten kann nur durch eine Person repräsentiert werden.

Stellvertretende Personen müssen für alle Aufgaben der primären Rolle fachlich und persönlich geeignet sein. Die stellvertretende Person muss so geschult oder ausgebildet werden, dass sie die primäre Rolle jederzeit und vor allem in einer Notsituation in vernünftigem Masse vertreten kann.

Art. 36 Sicherheitsverantwortliche der BK und der Verwaltungseinheiten

Absatz 1: Mit «verantwortlich» ist die persönliche Pflicht zur Rechenschaft gegenüber der vorgesetzten Stelle gemeint. Sie setzt voraus, dass der verantwortlichen Person Befugnisse – insbesondere finanziell – zustehen, Massnahmen zu veranlassen, zu überprüfen oder zu korrigieren. Davon abzugrenzen ist die Pflicht zur Durchführung von Aufsichtsmassnahmen. In diesem Fall ist die beauftragte Person für die Durchführung verantwortlich und einzig dafür rechenschaftspflichtig.

Absatz 2: Mit der Delegation der Sicherheitsverantwortung wird auch die persönliche Rechenschaftspflicht delegiert. Aus diesem Grund sollte die Delegation nachweisbar erfolgen (vgl. Erläuterungen Art. 8 Abs. 2 Bst. a).

Absatz 3 Buchstabe b: Grundsätzlich werden sämtliche wichtige Entscheide, welche die Informationssicherheit betreffen, von dieser Rolle getroffen.

Absatz 4: Die Beauftragung der Informationssicherheitsbeauftragten nach Artikel 37 kann zum Beispiel über interne Weisungen oder über die Festlegung von Jahreszielen im Sinne von Artikel 5 Absatz 2 erfolgen. Zum Begriff «Interessenkonflikt», vgl. ISG-Botschaft zu Artikel 82 Absatz 3.

Art. 37 Informationssicherheitsbeauftragte der Verwaltungseinheiten

Die Bezeichnung einer offiziellen Stellvertretung ist neu. Diese Rolle entspricht weitgehend dem heutigen Informatiksicherheitsbeauftragten der Verwaltungseinheiten (ISBO).

Art. 38 Informationssicherheit bei den Standarddiensten

Grundsätzlich hat diese Rolle bei den Standarddiensten die gleichen Aufgaben wie die Rolle der Informationssicherheitsbeauftragten der Verwaltungseinheiten nach Artikel 37.

Art. 39 Sicherheitsverantwortung der Departemente

Absätze 1 und 2: Die Steuerung und Überwachung der Informationssicherheit sind strategische Aufgaben und die Kernaufgaben der Departemente (vgl. Art. 38 RVOG, Erläuterungen zu Art. 5 Abs. 1).

Absatz 3: Diese Bestimmung erlaubt den Departementen mit einer mehr zentralen Organisation (wie das EDA), ihre internen Organisationsbedürfnisse im Rahmen der ISV umzusetzen.

Art. 40 Informationssicherheitsbeauftragte der Departemente

Die Bezeichnung einer offiziellen Stellvertretung ist neu (vgl. Art. 81 Abs. 1 ISG). Diese Rolle vereint die Rolle der heutigen Informatiksicherheitsbeauftragten (ISBD) und Informationsschutzbeauftragten der Departemente.

Buchstabe e: Weil die Rollen nach Artikel 37 und 40 eng zusammenarbeiten müssen, sollte die Rolle nach Artikel 40 bei der Wahl einer neuen Person für die Rolle nach Artikel 37 einbezogen werden.

Buchstabe f: Das Verfahren der heutigen Geheimaktenkontrolle wird unverändert übernommen.

Buchstabe g: Diese Rolle hat neu eine zusätzliche Aufgabe im Bereich der PSP. Details werden auf Weisungsebene festgelegt und die Rollenträger entsprechend geschult.

Buchstabe h: Heute müssen die jährlichen Berichte der ISBD dem NCSC zugestellt werden. Neu haben die Rollenträgerinnen und Rollenträger nach dieser Bestimmung der sicherheitsverantwortlichen Person des Departements nach Artikel 39 Bericht zu erstatten (vgl. Art. 14). Danach stellen Letztere den Bericht der Fachstelle des Bundes für Informationssicherheit zu, damit diese ihrerseits dem Bundesrat jährlich Bericht über den Stand der Informationssicherheit erstatten kann (vgl. Art. 83 Abs. 1 Bst. h ISG).

Art. 41 Fachstelle des Bundes für Informationssicherheit

Absatz 1: Die generellen Aufgaben der Fachstelle des Bundes für Informationssicherheit sind in 83 ISG und in Artikel 41 ISV zu finden; die kontextbezogenen Aufgaben in weiteren Bestimmungen der ISV (z. B. Vorgaben zum Management der Informationssicherheit nach Art. 16, weitere Vorgaben in verschiedenen Bereichen nach Art. 21, 29, 31, 34 und 35 Abs. 4).

Absatz 3: Die Konferenz der Informationssicherheitsbeauftragten nach Artikel 82 Absatz 2 Buchstabe c ISG berät die Fachstelle des Bundes für Informationssicherheit in allen Fragen der Vollzugskoordination und Fragen strategischer Bedeutung.

Absatz 4: Die Rolle der nationalen Sicherheitsbehörde wird neu der Fachstelle des Bundes für Informationssicherheit zugeordnet. Heute wird sie durch den Bereich Digitalisierung und Cybersicherheit VBS im Generalsekretariat des VBS wahrgenommen. Die Aufgaben und Kompetenzen gemäss Buchstaben d und f sind Gegenstand der völkerrechtlichen Verträge nach Artikel 87 ISG (vgl. ISG-Botschaft zu Art. 88, S. 3071; S. 3090).

8. Abschnitt: Kosten und Evaluation

Art. 42 Kosten

Die Verwaltungseinheiten tragen die Kosten ihrer eigenen Sicherheit. Diese Kosten müssen bereits bei der Planung von Vorhaben und Projekten berücksichtigt und ausgewiesen werden. Dies ist insbesondere für die Kosten der Massnahmen der Informatiksicherheit der Fall.

Art. 43 Evaluation

Vgl. ISG-Botschaft, Erläuterungen zu Artikel 89 ISG, Seite 3071.

9. Abschnitt: Bearbeitung von Personendaten

Die Artikel 44–46 regeln die Bearbeitung von Informationen und Personendaten im Rahmen des Managements der Informationssicherheit nach dieser Verordnung. Die Bewältigung von Sicherheitsvorfällen setzt die Bearbeitung von Daten über potenzielle Täterinnen oder Täter voraus, die in Verbindung mit administrativen oder strafrechtlichen Verfolgungen und Sanktionen stehen können und deshalb als besonders schützenswerte Personendaten im Sinne von Artikel 3 Buchstabe c DSG gelten. Die Datenschutzgesetzgebung verlangt dafür eine ausdrückliche Rechtsgrundlage auf Gesetzebene, die heute fehlt. Im Rahmen der laufenden Revision des ISG (vgl. Ziff. 3.1) wird die nötige formell-gesetzliche Grundlage geschafft.

Art. 44 Allgemeines

Absätze 1 und 2: Die Verwaltungseinheiten und deren Sicherheitsorgane können ohne gegenseitigen Informations- und Personendatenaustausch ihre Aufgaben nicht wahrnehmen. Zur Bearbeitung von besonders schützenswerten Personendaten im Rahmen des Vorfallmanagements: vgl. Erläuterungen zum 9. Abschnitt.

Art. 45 ISMS-Anwendung

Diese Bestimmung schafft die Rechtsgrundlage für den Einsatz von ISMS-Anwendungen, mit welchen die Aufgaben und Prozesse der ISV digitalisiert werden (vgl. Ziff. 3.8). Zur Bearbeitung von besonders schützenswerten Personendaten: vgl. Erläuterungen zum 9. Abschnitt.

Art. 46 Elektronische Formulardienste

Absatz 1: Ein Formulardienst ist eine kleine, einfache Anwendung, mit welcher Formulare elektronisch gefüllt und versandt werden. Die Formulardienste nach Absatz 1 dienen dazu, sogenannte Besuchsanträge («Request for Visit», Abs. 1 Bst. a), Sicherheitsermächtigungsbestätigungen (Abs. 1 Bst. b) und Betriebssicherheitsbescheinigungen im internationalen Verhältnis («Facility Security Clearances», Abs. 1 Bst. c) automatisiert auszustellen.

Absatz 2: Bei den Daten im Anhang 2 handelt es sich Personendaten, die ähnlich einem ESTA-Reisegenehmigungsprozess für Reisen in die USA verlangt werden. Die im Anhang 2 mit einem Stern (*) gekennzeichneten Daten werden an ausländische Behörden weitergegeben. Die datenschutzrechtlichen Bestimmungen zur Datenweitergabe ins Ausland (insbesondere Art. 16 Abs. 1 und Art. 17 nDSG) werden eingehalten. Ohne die Angabe dieser Daten erhält die antragstellende Person keinen Zugang zum klassifizierten Projekt im Ausland.

Absätze 3–6: Im Rahmen einer Sicherheitsmeldung können klassifizierte Informationen oder Personendaten bearbeitet werden. Mit dem Versand der Meldung gehen die Daten sofort in die ISMS-Anwendung, in welcher die Meldung und der Vorfall bearbeitet werden. Aus Informationssicherheits- und Datenschutzgründen dürfen die potenziell sensitiven Daten nicht länger als 24 Stunden im Formulardienst gespeichert werden. Zur Bearbeitung von besonders schützenswerten Personendaten im Rahmen des Vorfallmanagements: vgl. Erläuterungen zum 9. Abschnitt.

10. Abschnitt: Schlussbestimmungen

Art. 47 Aufhebung und Änderung anderer Erlasse

Die CyRV und die ISchV werden aufgehoben.

Art. 48 Übergangsbestimmungen

Nebst den Übergangsbestimmungen in dieser Bestimmung finden sich weitere im ISG, in der VPSP und VBSV. Mit den Übergangsbestimmungen soll das neue Recht innerhalb von sechs Jahren nach Inkraftsetzung systematisch und ordentlich geplant und umgesetzt werden können (vgl. auch Art. 90 ISG).

Art. 49 Inkrafttreten

Es wird noch geprüft, ob eine Teilinkraftsetzung notwendig ist.

Anhang 1

Das [zuständige Departement] wird den Anhang 1 aktuell halten.

Anhang 2

Vgl. Erläuterungen zu Artikel 46.

Anhang 3

Ziffer 1: Änderung der Verordnung vom 25. November 2020[22] über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (VDTI): Die CyRV wird durch die ISV ersetzt.

[22] SR **172.010.58**

Ziffer 2: Organisationsverordnung für das VBS vom 7. März 2003[23] (OV-VBS): Mit dem ISG und der ISV entfällt der Begriff der «militärischen Geheimhaltung». Die Koordinationsstelle für den Informationsschutz im Bund wird aufgelöst und ihre Aufgaben von der Fachstelle des Bundes für Informationssicherheit wahrgenommen.

Ziffer 3: Verordnung vom 24. Juni 2009[24] über internationale militärische Kontakte (VIMK): Mit dem ISG und seinen Ausführungsverordnungen müssen die relevanten Organe und Verordnungen aktualisiert werden.

4.2 Änderung der Verordnung über Identitätsverwaltungssysteme und Verzeichnisdienste des Bundes (IAMV)

Ingress

Mit den Artikeln 24–26 ISG wurde eine spezifische formell-gesetzliche Grundlage für die bestehende IAMV geschaffen, indem die wichtigsten Bestimmungen der Verordnung auf Gesetzesstufe gehoben wurden. Bisher stützte sich die Verordnung auf die Organisationskompetenz des Bundesrats und indirekt auf die gesetzlichen Grundlagen sämtlicher an die IAM-Systeme angeschlossenen Systeme. Gestützt auf Artikel 20 Absatz 2 ISG wird es zudem unter bestimmten Voraussetzungen zulässig sein, in IAM-Systemen biometrische Daten zu bearbeiten. Diese gelten nach dem nDSG als besonders schützenswerte Personendaten (BBl 2020 7639, Art. 5 Bst. c Ziff. 4). Somit wird der Grundsatz relativiert, wonach in IAM-Systemen keine besonders schützenswerten Personendaten bearbeitet werden dürfen (Art. 11 Abs. 3). Weiterhin besteht sodann die Möglichkeit, gestützt auf spezifische Gesetzesbestimmungen ausserhalb des ISG, besonders schützenswerte Personendaten in IAM-Systemen zu bearbeiten. Persönlichkeitsprofile betragen im nDSG keine relevante Grösse mehr und brauchen daher nicht mehr erwähnt zu werden. Ein Profiling im Sinne von Artikel 5 Buchstabe f nDSG findet in IAM-Systemen und Verzeichnisdiensten nicht statt, da diese nicht dazu dienen, persönliche Aspekte von Personen zu *bewerten*.

Art. 2 Geltungsbereich

Der in Artikel 2 Absatz 2 Buchstabe b ISG verwendete Begriff «Bundesverwaltung» umfasst sowohl die zentrale als auch die dezentrale Bundesverwaltung (vgl. ISG-Botschaft, S. 3012), weshalb der Geltungsbereich neu auf die Verwaltungseinheiten der dezentralen Bundesverwaltung erweitert werden soll, sofern sie Zugriff auf Informatiksysteme der zentralen Bundesverwaltung haben.

Die Inhalte des heutigen Absatzes 2 stellen keine abschliessende Positivliste dar und können daher ersatzlos gestrichen werden (wenn sich eine Behörde oder Stelle freiwillig verpflichten will, die IAMV einzuhalten, so ist dies ohne explizite rechtliche Grundlage möglich).

Art. 3 Abs. 1

Bisher werden Identitäten nachgelagerten IAM-Systemen oder Identitätsspeichern nur passiv zum Selbstbezug angeboten – diese konsumieren die Identitäten nach eigenem Takt, Rhythmus und Bedarf. Im Rahmen von proaktiveren Schutzmassnahmen (z.B. umgehende Berechtigungsveränderungen oder Notfallsperrungen) kann man sich nicht mehr auf den Durchsetzungszeitpunkt der Anmeldung an Anwendungen verlassen, sondern es müssen die nachgelagerten, mit IAM-versorgten Systeme, proaktiv mit diesen sicherheitsrelevanten Informationen versorgt werden. Diese eine neue Art der Versorgung ist wichtig und soll daher in der IAMV verankert werden. Die heutige Formulierung, die vorsieht, dass ein IAM-System die Daten nachgelagerten Systemen oder anderen IAM-Systemen nur «auf Anfrage» zur Verfügung stellt, wird daher entsprechend angepasst, indem die Umschreibung «auf Anfrage» gestrichen wird.

Art. 5 IAM-Systeme

Absatz 1: Neben den bereits heute in der IAM aufgeführten verantwortlichen Bundesorganen werden die weiteren verantwortlichen Bundesorgane (Bst. c und g) von IAM-Systemen aufgeführt.

Absatz 2: Aktuell erfolgt keine Kontrolle der Bearbeitung der Personendaten in IAM-Systemen. Artikel 26 Buchstabe e ISG verlangt nun – im Übrigen nicht nur bezüglich der IAM-Systeme – explizit, dass eine periodische Kontrolle der Bearbeitung von Personendaten durch eine externe Stelle vorgesehen wird. Entsprechend wird in Artikel 5 ein zusätzlicher Absatz eingefügt.

[23] SR **172.214.1**
[24] SR **510.215**

Absatz 3: Die IAMV ist aufgrund von Artikel 84 Absatz 3 ISG auch auf die verpflichteten Behörden nach Artikel 2 Absatz 1 Buchstaben a und c–e ISG anwendbar, soweit diese keine eignen Bestimmungen erlassen. Damit dieses Konstrukt funktioniert, müssen die anderen verpflichteten Behörden mindestens regeln, wer in ihrem Bereich die datenschutzrechtliche Verantwortung innehat.

Absatz 4: Aufgrund der neuen Absätze 2 und 3 wird der heutige Absatz 2 inhaltlich unverändert zu Absatz 4.

Art. 11 Abs. 2 und 3

Die heutigen Absätze 2 und 3, wonach in den IAM-Systemen keine Persönlichkeitsprofile und ohne besondere rechtliche Grundlage auch keine besonders schützenswerten Personendaten bearbeitet werden dürfen, sind einerseits aufgrund von Artikel 20 Absatz 2 ISG und andererseits aufgrund der Totalrevision des nDSG zweifach zu überarbeiten (vgl. die Ausführungen unter Ziff. 3.4). Erstens tritt an die Stelle des Verbots der Bearbeitung von Persönlichkeitsprofilen ein Verbot des Profiling (vgl. Art. 5 Bst. f nDSG). Zweitens gelten biometrische Daten, die eine Person eindeutig identifizieren, neu pauschal als besonders schützenswerte Personendaten. Für ihre Bearbeitung wird aber in Artikel 20 Absatz 2 ISG eine allgemeine Grundlage geschaffen. Solche biometrischen Daten dürfen daher nach dem Anhang (Bst. a Ziff. 11) neu grundsätzlich in allen IAM-Systemen bearbeitet werden, in denen es zur risikogerechten Identifizierung erforderlich ist.

Art. 13 Abs. 4

In Buchstabe a wird der Klarheit halber explizit festgehalten, dass die fragliche Rechtsgrundlage (auch) die Bearbeitung der bereitzustellenden Daten vorsehen muss.

Art. 14 Abs. 2

Diese Bestimmung bleibt materiell unverändert, jedoch ist der Verweis nicht mehr auf Artikel 2*a* des Bundesgesetzes vom 3. Oktober 2008[25] über die militärischen Informationssysteme (MIG), sondern neu auf das ISG zu machen.

Gliederungstitel vor Art. 18 sowie Art. 18 Abs. 1 und 2

Informationssicherheit und die Einhaltung derer Vorgaben sollen nicht ausschliesslich für IAM-Systeme selbst gelten, sondern ebenso für Verzeichnisdienste anwendbar sein. Dies gilt auch für bundesexterne Anbieter von Verzeichnisdiensten, insbesondere wenn diese Anbieter nicht bereits ein IAM-System betreiben. Der Verordnungstext wird daher entsprechend ergänzt.

Art. 20 IAM-Gesamtsystem

Gemäss heutigem Artikel 20 können die IAM-Systeme der Bundesverwaltung untereinander sowie mit den IAM-Systemen der Parlamentsdienste oder der Armee in optimaler Art untereinander verbunden werden, um eine effiziente Aufgabenteilung zu ermöglichen. Dies bedeutet auch, dass in der Art einer Föderation Benutzerdaten untereinander ausgetauscht werden können. Neu sollen die genannten IAM-Systeme auch mit den IAM-Systemen nach Artikel 21 verbunden werden können, weshalb Artikel 20 materiell entsprechend ergänzt wird. Formell neu ist, dass sämtliche IAM-Systeme ausserhalb der Bundesverwaltung (externe IAM-Systeme), also auch die bisher in Artikel 20 aufgeführten IAM-Systeme der Parlamentsdienste und der Armee, zusammen in Artikel 21 aufgelistet werden.

Art. 21 Anschluss externer IAM-Systeme: Voraussetzungen

Einleitungssatz: Wenn ein externes IAM-System nach Artikel 21 mit den IAM-Systemen der Bundesverwaltung, der Parlamentsdienste oder der Armee verbunden werden sollen, ist es insbesondere aus Sicherheitsgründen zwingend, dass sich die fraglichen Betreiberinnen und Betreiber der IAMV unterwerfen. Der Einleitungssatz wird daher entsprechend ergänzt.

Buchstaben a und b: Neu werden in der Aufzählung auch die bisher in Artikel 20 aufgeführten IAM-Systeme der Parlamentsdienste und de Armee aufgelistet.

Die Buchstaben c–f entsprechen den heutigen Buchstaben a–d.

[25] SR **510.91**

Anhang

Gestützt auf Artikel 20 Absatz 2 ISG werden biometrische Daten, nicht nur für Personen, die in von der Armee betriebenen Systemen geführt, sondern für sämtliche in IAM-Systemen geführten Personen, bearbeitet (heute ist dies gestützt auf Art. 2*a* MIG nur für Systeme der Armee möglich). Die biometrischen Daten, aktuell unter Buchstabe g geführt, werden daher neu in Buchstabe a integriert. Buchstabe g kann somit aufgehoben werden.

Biometrische Daten dürfen jedoch nicht systematisch in allen IAM-Systemen geführt und für jegliche Anwendungsfälle eingesetzt werden. Vielmehr ist für jedes IAM-System und für jedes Anwendungsszenario zu prüfen, ob der Einsatz biometrischer Daten zur risikogerechten Identifizierung von Personen erforderlich ist. Zudem sind die biometrischen Daten nach dem Wegfall der Zugangsberechtigung zu vernichten (vgl. Art. 20 Abs. 3 ISG und Art. 14 Abs. 2 IAMV).

Zudem werden die Spalten «Verzeichnisdienste» und «IAM-Systeme mit Personen nach Artikel 8 und 9 Buchstabe a» zusammengelegt. Eine Differenzierung zwischen Verzeichnisdiensten und den fraglichen IAM-Systemen hat sich in der Vergangenheit als extrem hinderlich im Angebot von IAM-Leistungen an Verwaltungsprozesse erwiesen und so sollen künftig alle Informationsbezüger bei Anbindung an IAM-Services die kompletten Bearbeitungs- und Verarbeitungsreglemente offenlegen (so wie dies bis anhin nur für die IAM-Systeme galt).

Schliesslich werden – dem Wortlaut des ISG entsprechend – in Buchstabe f (Einleitungssatz und Ziff. 2) zwei sprachliche Anpassungen vorgenommen.

4.3 Verordnung über die Personensicherheitsprüfungen (VPSP)

Titel

Unter dem Begriff «Personensicherheitsprüfung» werden neben den Personensicherheitsprüfungen (PSP) nach dem ISG alle Prüfungen, Beurteilungen und Kontrollen nach anderen Gesetzen zusammengefasst, auf welche das Verfahren der PSP nach dem ISG direkt oder sinngemäss anwendbar ist.

Ingress

Der Ingress verweist auf sämtliche Gesetzesnormen, die dem Bundesrat eine Regelungskompetenz im Bereich der PSP erteilen.

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Gegenstand

Absätze 1 und 2: Mit der VPSP soll eine Verordnung für alle Vollzugskompetenzen nach Artikel 48 ISG zu den PSP nach dem ISG und den Prüfungen, Beurteilungen und Kontrollen nach anderen Gesetzen erlassen werden.

Absatz 3: Der Bundesrat hat als verpflichtete Behörde nach Artikel 2 Absatz 1 ISG spezifische Vollzugsaufgaben für die Bundesverwaltung.

Art. 2 Geltungsbereich

Artikel 2 ISG wird durch den Bundesrat in Artikel 2 der ISV konkretisiert. Diese Bestimmung ist daher auch für den Geltungsbereich der VPSP massgebend.

2. Abschnitt: Funktionenlisten

Art. 3 Zuordnung

Absätze 1–3: Für jede Art von PSP wird eine eigene Funktionenliste als Anhang zur Verordnung erlassen. Gemäss Artikel 41*b* Absatz 2 des Ausländer- und Integrationsgesetzes vom 16. Dezember 2005[26] und 6*a* Absatz 2 des Ausweisgesetzes[27] vom 22. Juni 2001 könnten auch für bestimmte Personen im Bereich der Ausstellung von Ausweisen Sicherheitsprüfungen im Sinne von Artikel 6 der heutigen PSPV durchgeführt werden. In der VPSP sollen bewusst keine Funktionenlisten dafür geführt werden. Bei zwingendem Bedarf an PSP wären diese über ein Betriebssicherheitsverfahren bei den entsprechenden Unternehmen abgedeckt.

[26] SR **142.20**
[27] SR **143.1**

Die Listen dürfen keine Funktionen enthalten, welche die strikten Voraussetzungen der Artikel 10–14 VPSP nicht einhalten.

Die verpflichteten Behörden nach Artikel 2 ISG, die nicht in den Zuständigkeitsbereich des Bundesrates fallen (beispielsweise die Bundesanwaltschaft), müssen ihre Funktionenlisten selber erlassen.

Absatz 4: Dieser Absatz entspricht inhaltlich der geltenden Regelung von Artikel 1 Absatz 3 PSPVK.

Art. 4 Änderung

Um die Anzahl der Prüfungen im angestrebten Rahmen zu behalten, bedarf es bei der Erstellung und Nachführung der Funktionenlisten, in denen die zu prüfenden Funktionen aufgelistet sind, einer besseren Kontrolle der Rechtmässigkeit der Einträge als heute. Das VBS soll deshalb die Funktionenlisten zentral bewirtschaften. Das VBS soll deshalb die Funktionenlisten zentral bewirtschaften und sie auf Antrag der Departemente und die BK laufend aktualisieren. Dabei soll es die Fachstelle des Bundes für Informationssicherheit beiziehen.

Art. 5 Veröffentlichung, Aufbewahrung und Bekanntgabe

Zur Sicherheitsempfindlichkeit der Funktionenlisten, vgl. Ziff. 3.5 Bst. d. Jene Stellen und Personen, die für ihre Aufgabenerfüllung Einsicht in nicht veröffentlichte Funktionenlisten haben müssen, sollen diese über das VBS einsehen können. Es handelt sich dabei insbesondere um die einleitenden Stellen und die Sicherheitsorgane nach der ISV.

Art. 6 Aktualitätsprüfung

Absatz 1: Die Prüfung der Richtigkeit der Funktionenlisten erfordert einen erheblichen Aufwand. Es besteht aber ein klarer Bedarf dafür, die Funktionenlisten aktuell zu halten und einmal erfolgte Einreihungen von Funktionen zu hinterfragen, damit immer nur jene Personen geprüft werden, für deren Funktion eine Prüfung aufgrund des potentiellen Risikos erforderlich ist. Es soll daher der pragmatische Ansatz festgelegt werden, die Funktionenlisten mindestens einmal pro Legislatur generell und bei Reorganisationen oder Aufgabenänderungen spezifisch zu überprüfen.

Absatz 2: Aufgrund bisheriger Erfahrungen muss sichergestellt werden, dass die Prüfung der Richtigkeit der Funktionenlisten auch tatsächlich stattfindet. Es soll daher dem VBS darüber Bericht erstattet werden müssen. Ergibt sich bei der Prüfung der Richtigkeit der Funktionenlisten ein Änderungsbedarf für die Funktionenlisten, sind diese entsprechend zu überarbeiten.

Art. 7 Ausserordentliche Prüfung

Falls eine Funktion die Kriterien für eine Prüfung erfüllt, aber noch nicht in die entsprechende Funktionenliste aufgenommen wurde, kann gestützt auf Artikel 29 Absatz 3 ISG eine Prüfung durchgeführt werden, sofern die verpflichtete Behörde zustimmt. Für die Bundesverwaltung soll, die entsprechende Entscheidkompetenz für eine Ausnahmeprüfung an das VBS delegiert werden, welches die Fachstelle des Bundes für Informationssicherheit konsultiert. Die Funktionenlisten sind entsprechend nachzuführen. Die anderen verpflichteten Behörden regeln die Zuständigkeiten selbst.

Art. 8 Prüfung bei kantonalen Angestellten und Dritten

Absatz 1: Die Festlegung der Funktionen von Angestellten eines Kantons, die einer Prüfung nach Artikel 29 Absatz 1 Buchstabe b ISG unterstehen, ist grundsätzlich Sache der Kantone. Damit eine einheitliche Handhabung sichergestellt werden kann, soll das VBS hier jedoch eine Steuerungsfunktion erhalten. Dabei konsultiert es die Fachstelle des Bundes für Informationssicherheit.

Absatz 2: Die Funktionen der Dritten, die für eine verpflichtete Behörde oder Organisation einen Auftrag ausführen, der die Ausübung einer sicherheitsempfindlichen Tätigkeit einschliesst, können nicht zum Voraus bestimmt werden, sondern ergeben sich nach den Notwendigkeiten der einzelnen Aufträge. Damit auch hier die Notwendigkeit der Prüfung gewährleistet ist, sollen die Entscheide zentralisiert erfolgen.

Art. 9 Ausserordentliche Zuverlässigkeitskontrolle des Eidgenössischen Nuklearsicherheitsinspektorats

Dieser Artikel entspricht inhaltlich der geltenden Regelung von Artikel 5 PSPVK.

4. Abschnitt: Prüfstufen

Die Zuordnung der Prüfung der Vertrauenswürdigkeit nach dem Asylgesetz zur Prüfstufe Grundsicherheitsprüfung wird bereits in Artikel 29*a* des Asylgesetzes vom 26. Juni 1998[28] (AsylG) festgelegt und ist daher in der Verordnung nicht mehr zu regeln.

Art. 10 Personensicherheitsprüfung nach dem ISG

Absatz 1 Buchstabe a: Mit «Bearbeitung» ist jeder Umgang mit Informationen, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Speichern, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Löschen oder Vernichten von Informationen gemeint. Dabei geht es um die regelmässige Bearbeitung von klassifizierten Informationen. Falls nur Ausnahmsweise solche Informationen bearbeitet werden und die Bearbeitung von klassifizierten Informationen nicht zur eigentlichen Funktion gehört, ist eine PSP nicht erforderlich.

Absatz 1 Buchstabe b: Mit «die Verwaltung, der Betrieb, die Wartung oder die Überprüfung von Informatikmitteln» werden alle Tätigkeiten nach Artikel 5 Buchstabe b ISG erfasst, die mit besonderen Zugriffsrechten auf die Informatikmittel des Bundes verbunden oder bei deren Ausübung Personen in der Lage sind, beispielsweise durch Datendiebstahl oder Sabotage, die Interessen nach Artikel 1 Absatz 2 ISG erheblich zu beeinträchtigen. Ob die Anwender von Informatikmitteln eine sicherheitsempfindliche Tätigkeit ausüben, entscheidet sich allein aufgrund der Inhalte der bearbeiteten Informationen. Erfasst werden folglich vor allem Administratoren und Anwendungsverantwortliche der Systeme. Der Begriff «Betrieb» bezieht sich auf die Aktivität der Leistungserbringerinnen im Sinne von Artikel 19 ISG. Er ist klar vom Ausdruck ein Informationssystem betreiben abzugrenzen, der in der Datenschutzgesetzgebung verwendet wird, um eigentlich den Einsatz eines Informationssystems durch die Leistungsbezügerin zu regeln (vgl. z. B. Art. 24 Abs. 1 ISG). Sicherheitsempfindliche Tätigkeiten im Rahmen der Entwicklung oder des Baus von Informationssystemen sind im Buchstaben b als Teil der Verwaltung und des Betriebs inbegriffen.

Absatz 1 Buchstabe c: Die Ausscheidung von Räumen beziehungsweise Bereichen als Sicherheitszone stellt eine physische Massnahme der Informationssicherheit dar, insbesondere zum Schutz von Serverräumen oder von bestimmten Führungsräumen. Eine Sicherheitszone muss entsprechend geschützt werden. Personen, die Zugang zu solchen Sicherheitszonen haben müssen, sollen daher einer Grundsicherheitsprüfung unterstehen.

Absatz 1 Buchstabe d: Sofern völkerrechtliche Verträge eine Prüfung vorsehen, richtet sich die Prüfstufe nach den entsprechenden Vorgaben des Vertrags. Enthält der Vertrag keine spezifische Regelung, erfolgt die Prüfung immer nur in der Prüfstufe Grundsicherheitsprüfung.

Absatz 2 Buchstaben a und b: Vgl. Erläuterung zu Absatz 1 Buchstaben a und b.

Absatz 2 Buchstaben c und d: Personen, die für den Nachrichtendienst des Bundes (NDB) oder seine Aufsichtsbehörde, den militärischen Nachrichtendienst und für das Zentrum elektronische Operationen der Führungsunterstützungsbasis sicherheitsempfindliche Tätigkeiten ausüben, tun dies regelmässig in höchst sensitiven Bereichen. Ihre Tätigkeiten sollen daher der Prüfstufe erweiterte Personensicherheitsprüfung zugeordnet sein.

Absatz 2 Buchstabe e: Vgl. Erläuterungen zu Absatz 1 Buchstabe d.

Art. 11 Prüfung der Vertrauenswürdigkeit nach dem BPG

Absatz 1 Buchstabe a: Bei den hoheitliche Tätigkeiten von im Ausland eingesetztem Personal und von der Versetzungspflicht unterstehendem Personal des EDA (vgl. Art. 3 Bst. a und b der Verordnung des EDA vom 20. September 2022[29] zur Bundespersonalverordnung) können wesentliche Interessen des Bundes erheblich beeinträchtigt werden. Personen, die solche Tätigkeiten ausüben, sollen auf Stufe Grundsicherheitsprüfung geprüft werden.

Absatz 1 Buchstabe b: Gemäss der derzeit geltenden Bewertungsmatrix des Risikomanagements des Bundes entspricht eine potentielle finanzielle Auswirkungsdimension von 50–500 Millionen Franken der Auswirkung «erheblich».

Absatz 1 Buchstabe c: Die Spannweite von Strafverfolgungs- und polizeilichen Aufgaben kann je nach Auslegung dieser Begriffe sehr gross sein. Der Anwendungsbereich dieses Prüfgrundes ist

[28] SR **142.31**
[29] SR **172.220.111.343.3**

daher auf jene Aufgaben zu beschränken, die die öffentlichen Interessen des Bundes erheblich gefährden können.

Absatz 1 Buchstaben d: Personen, die im engsten Umfeld einer Departementsvorsteherin oder eines Departementsvorstehers oder der Bundeskanzlerin oder dem Bundeskanzler tätig sind, können bei unsachgemässer Ausübung ihrer Funktion regelmässig einen erheblichen Schaden verursachen. Sie sollen daher ausnahmslos einer Grundsicherheitsprüfung unterstehen.

Absatz 2 Buchstaben a–c: Funktionsträgerinnen und Funktionsträger, für die der Bundesrat nach Artikel 2 Absatz 1 oder der Departementsvorsteher oder die Departementsvorsteherin nach Artikel 1bis der Bundespersonalverordnung vom 3. Juli 2001[30] (BPV) für die Begründung, Änderung und Beendigung des Arbeitsverhältnisses zuständig ist, erfüllen regelmässig mindestens einen der Prüfgründe nach Artikel 20*b* Absatz 1 Buchstaben a und b BPG. Dies trifft ebenfalls bei Funktionsträgerinnen und Funktionsträger nach Artikel 2 Absatz 1 Buchstabe e BPG zu. Aufgrund des damit verbundenen hohen Reputationsschadens bei Verfehlungen dieser Funktionsträgerinnen und Funktionsträger sollen sie der erweiterten Personensicherheitsprüfung unterstehen.

Absatz 2 Buchstabe d: Gemäss der derzeit geltenden Bewertungsmatrix des Risikomanagements des Bundes entspricht eine potentielle finanzielle Auswirkungsdimension von mehr als 500 Millionen Franken der Auswirkung «hoch» und bei mehr als einer Milliarde Franken als «sehr hoch».

Absatz 2 Buchstabe e: Tätigkeiten der Angestellten der Fachstellen PSP nach Artikel 16 Absatz 1 sollen ebenfalls der erweiterten Personensicherheitsprüfung unterzogen werden, damit deren Glaubwürdigkeit gegenüber den zu prüfenden Personen gewährt ist.

Art. 12 Prüfungen nach dem Militärgesetz vom 3. Februar 1995[31] (MG)

Absatz 1 Buchstabe a: Nicht jede normale Tätigkeit von Angehörigen der Armee in Uniform im Ausland fällt unter den Begriff der «hoheitliche Vertretung» der Schweiz. Die rein optische Repräsentation der Schweiz oder Tätigkeiten im Rahmen von internationalen Truppenkontingenten sollen nicht für eine Prüfung der Vertrauenswürdigkeit genügen. Erforderlich sind Tätigkeiten, die hoheitliche Entscheidbefugnisse mit Aussenwirkung in Vertretung der Schweiz beinhalten.

Absatz 1 Buchstabe b: Vgl. Erläuterungen zu Artikel 11 Absatz 2 Buchstabe b.

Absatz 1 Buchstabe c: Für den Entscheid, ob ein Stellungspflichtiger nicht rekrutiert beziehungsweise ein Angehöriger der Armee degradiert oder aus der Armee ausgeschlossen werden soll, ist im Bedarfsfall eine Grundsicherheitsprüfung ausreichend.

Absatz 2: Heute kann bei allen Anwärterinnen und Anwärtern ungeachtet eines materiellen Prüfgrundes eine Personensicherheitsprüfung durchgeführt werden. Diese Möglichkeit entfällt mit der neuen VPSP. Neu dürfen diese nur geprüft werden, wenn ein materieller Prüfgrund nach dem ISG oder dem MG vorhanden ist. Hat die betroffene Person bereits eine gültige PSP und ist sie Anwärterin oder Anwärter auf eine Funktion, die eine PSP voraussetzt, so kann die PSP frühzeitig wiederholt werden, sofern die Mindestfrist nach Artikel 43 Absatz 1 ISG abgelaufen ist.

Art. 13 Zuverlässigkeitskontrollen nach dem Kernenergiegesetz vom 21. März 2003[32]

Dieser Artikel entspricht inhaltlich der geltenden Regelung nach Artikel 3 PSPVK.

Art. 14 Prüfungen der Vertrauenswürdigkeit nach dem StromVG

In Anlehnung an die nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022 sind kritische Informationen alle Informationen, die essenziell für das Funktionieren der Versorgungssicherheit, der kritischen Applikationen oder der kritischen Infrastrukturen sind. Höchstkritische Informationen sind alle Informationen, die höchst-essenziell für das Funktionieren der Versorgungssicherheit, der kritischen Applikationen oder der kritischen Infrastrukturen sind.

5. Abschnitt: Durchführung

Im Rahmen der Vorarbeiten zum vorliegenden Verordnungsentwurf wurde auch angeregt, für die Dauer der Beurteilung des Sicherheitsrisikos Maximalfristen vorzusehen, damit die Ergebnisse innert praktikabler Frist vorliegen. Darauf soll aufgrund früherer Erfahrungen mit solchen Fristen be-

[30] SR **172.220.111.3**
[31] SR **510.10**
[32] SR **732.1**

wusst verzichtet werden. Die Dauer der Beurteilung ist massgeblich beeinflusst von der Erhältlichkeit der zu erhebenden Daten und von deren tatsächlichem Inhalt. Eine absolute Frist würde, insbesondere kurz angesetzte Fristen, zu vermehrtem Ergehen von Feststellungserklärungen führen, weil Anzeichen auf Risiken nicht vertieft geklärt werden könnten oder die Daten nicht rechtzeitig vorliegen.

Art. 15 Einleitende und entscheidende Stellen

Absatz 1: Für die Bundesverwaltung sollen die Departemente und die BK die für ihre Organisation geeignetste Kompetenzzuordnung selber festlegen können.

Absatz 3: Dieser Absatz entspricht inhaltlich den bisherigen Artikeln 2 Absatz 2 und 4 Absatz 1 PSPVK.

Absatz 5: Damit die Fachstellen PSP ihre Arbeit effizient erledigen können, müssen sie wissen, wer bei den einzelnen Behörden für die Einleitung von Prüfungen und den Entscheid über die Ausübung der Funktion zuständig ist.

Art. 16 Fachstellen PSP

Am bewährten System von zwei Fachstellen PSP mit unterschiedlichen Zuständigkeiten soll festgehalten werden.

Die Fachstelle PSP BK soll nach Artikel 16 Absatz 2 Buchstabe d die «Funktionen des Generalsekretariats VBS mit Führungsaufgaben gegenüber der Fachstelle PSP VBS» überprüfen. Damit sind die Generalsekretärin beziehungsweise der Generalsekretär, deren oder dessen Stellvertreterin beziehungsweise Stellvertreter sowie die Leiterin beziehungsweise der Leiter der Fachstelle PSP VBS gemeint. Neben diesen drei Funktionen des GS-VBS überprüft die Fachstelle PSP BK keine weiteren Funktionen unter Buchstabe d.

Art. 17 Überprüfung der Voraussetzungen für die Prüfung

Für die Beurteilung der Sicherheitsempfindlichkeit der Funktionen sind die verpflichteten Behörden verantwortlich. Für die Fachstellen PSP sind die Funktionenlisten daher verbindlich. Sie können nicht bei jeder eingeleiteten PSP prüfen, ob die Funktion tatsächlich sicherheitsempfindlich ist. Der damit verbundene Aufwand wäre unverhältnismässig. Hingegen können und sollen sie prüfen, ob die Prüfungen korrekt eingeleitet wurden. Es ist im Übrigen Sache der einleitenden Stelle zu belegen, dass eine Einwilligung der zu prüfenden Person vorliegt und diese Einwilligung den Anforderungen an Artikel 4 Absatz 5 DSG genügt.

Art. 18 Mitwirkung

Die ganze Sicherheitsprüfung wäre illusorisch, wenn Fragen nach Alkohol- oder Betäubungsmittelmissbrauch, nach persönlichen Schulden, nach Nebenbeschäftigungen und ähnlichem unter Berufung auf die Grundrechte nicht beantwortet werden müssten und entsprechende Erkenntnisse aufgrund dessen nicht in die Beurteilung des Sicherheitsrisikos einfliessen würden. Im Rahmen der Mitwirkungspflicht hat die zu prüfende Person daher an der Sachverhaltserhebung mitzuwirken. Es bleibt der zu prüfenden Person unbenommen, bestimmte Fragen nicht beantworten zu wollen. Es ist dann aber Aufgabe der Fachstellen, die Auskunftsverweigerung oder auch die Verweigerung, weitere Dokumente wie Arztberichte und Drogentests einzureichen, zu würdigen, da ein gewisser Spielraum für Fragen zur persönlichen Geheimsphäre bestehen muss. Dabei sind allfällige gesetzliche Geheimnispflichten der zu prüfenden Person zu berücksichtigen.

Art. 19 Datenerhebung

Absatz 1: Die Datenbankabfragen erfolgen grundsätzlich für beide Fachstellen PSP über die FS PSP VBS. Die Fachstellen PSP müssen nicht unbedingt auf alle verfügbaren Mittel zugreifen, um das Risiko zu beurteilen. Dies ist insbesondere bei der erweiterten Prüfung wichtig, weil die Reduktion der Prüfstufen nicht dazu führen soll, dass die Kosten der PSP massiv erhöht werden. Es soll daher auch bewusst darauf verzichtet werden, festzulegen, wann welche Daten erhoben und bearbeitet werden müssen. Die Fachstellen PSP können am besten beurteilen, welche Daten für ihre Risikobeurteilungen notwendig sind.

Absätze 2 und 3: Die persönliche Befragung nach Artikel 34 Absatz 2 Buchstabe d ISG dient dazu, Sachverhalte anzusprechen, die aus den übrigen Datenerhebungen nicht oder nur unklar hervorgehen. Sie kann auch ohne Anhaltspunkte für ein Sicherheitsrisiko durchgeführt werden und ist im Befragungsumfang nicht eingeschränkt. Aufgrund des mit dieser Befragung einhergehenden

Aufwands ist sie auf möglichst wenige Funktionen zu beschränken. Die Aufzählung ist daher abschliessend. Bei allen aufgeführten Funktionen werden interne und externe Mitarbeitende gleichgesetzt. Die Befragung ist bei einer ordentlichen Wiederholung der Prüfung nach Artikel 26 nicht unbedingt notwendig, wenn sich die Risikolage kaum geändert hat.

Absatz 4: Zur Abklärung besonderer sicherheitsrelevanter Umstände oder zum Erhalt ergänzender Daten über einen längeren Zeitraum können die Fachstellen PSP auch Drittpersonen befragen. Absatz 4 nennt in seinen Buchstaben a–c die aus der bisherigen Praxis bekannten wichtigsten Personengruppen. Daneben gibt es je nach Fall andere Personen, die über wertvolle Informationen verfügen (beispielsweise Familienangehörige oder frühere Geschäftspartner). Diese werden mit einer allgemeinen Formulierung in Buchstaben d zusammengefasst. Verschiedentlich wurde angeregt, Dritte, die befragt werden dürfen, mit der Verordnung zu einer wahrheitsgemässen Auskunft zu verpflichten. Die gesetzlichen Grundlagen sehen jedoch keine Antwortpflicht vor. Die betroffene Drittperson kann also jederzeit auf die Erteilung jeglicher Auskunft verzichten.

Art. 20 Amtshilfe

Die Fachstellen PSP erheben nicht alle Daten selbstständig. Dies betrifft insbesondere Daten, die im Ausland erhoben werden. Diese Erhebung erfolgt in der Regel über das fedpol und den NDB. Nur diese Stellen sind in der Lage, die Zuverlässigkeit der Daten und Datenquellen zu würdigen.

Art. 21 Zusammenlegung von Prüfverfahren

Funktionen umfassen verschiedenste Tätigkeiten, die unterschiedliche Prüfgründe erfüllen können. Ist eine Person aufgrund mehrerer Prüfgründe zu prüfen, sollen die Prüfungen aus verfahrensökonomischen Gründen zusammengefasst werden. Ist eine Person aufgrund mehrerer Prüfgründe durch beide Fachstellen PSP zu prüfen, soll nur die Fachstelle PSP BK die Prüfung durchführen. Der Grund für die Fachstelle PSP BK liegt in Artikel 16 Absatz 2, wonach eine abschliessende Liste der Funktionen besteht, die eingehalten werden muss. Durch die Zusammenlegung lässt sich unnötiger Mehraufwand vermeiden. Die Prüfungsergebnisse sollen für den jeweiligen Prüfgrund separat ausgewiesen werden.

Art. 22 Auflagen

Die Fachstellen PSP empfehlen den entscheidenden Stellen geeignete Auflagen, um das von der Fachstellen PSP beurteilte Sicherheitsrisiko auf ein tragbares Mass zu reduzieren. Die entscheidenden Stellen sind nicht an diese Empfehlungen gebunden. Sie können die empfohlenen Auflagen übernehmen, andere vorsehen oder verzichten.

Art. 23 Mitteilung

Absatz 1: Unterstehen Personen aufgrund verschiedener Prüfgründe einer Prüfung, die nicht gleichzeitig erfolgt, sollen risikorelevante Feststellungen in einer späteren Prüfung den entscheidenden Stellen der früheren Prüfung mitgeteilt werden können, damit im Bedarfsfall Sicherheitsmassnahmen ergriffen werden können. Dies ist insbesondere für Prüfungen nach Artikel 113 MG wichtig, welchen alle Angehörigen der Armee unterstehen. Wird im Rahmen einer anderen Prüfung ein Risiko in Bezug auf die Armeewaffe festgestellt, so dürfen die Fachstellen PSP der zuständigen militärischen Behörde die Erklärung mitteilen.

Absatz 2: Bei einem begründeten Sicherheitsvorbehalt und bei Dringlichkeit dürfen die Fachstellen PSP zur Gefahrenprävention die zuständigen Stellen über ihre Erkenntnisse informieren, bevor das Verfahren abgeschlossen ist. Die betroffene Stelle kann daraufhin vorsorgliche Sicherheitsmassnahmen treffen. Dies ist insbesondere bei der maximal drei Tage dauernden Rekrutierung von Stellungspflichtigen von Bedeutung. Sicherheitsvorbehalte (beispielsweise früherer Drogenkonsum) können insbesondere auch für die Beurteilung der Militärdiensttauglichkeit durch die Ärzte und Psychologen der Rekrutierung von wesentlicher Bedeutung sein.

6. Abschnitt: Folgen der Erklärung

Art. 24 Ausübung der Tätigkeit

Absatz 1: Die entscheidende Stelle trägt die Verantwortung für die Tätigkeiten der geprüften Person und entscheidet deshalb über die Ausübung der Tätigkeit. Allfällige von den Fachstellen PSP empfohlenen Auflagen sind für die entscheidenden Stellen nicht verbindlich (vgl. Art. 22). Sie können die empfohlenen Auflagen übernehmen, andere vorsehen oder völlig verzichten. Wird jedoch die Ausübung der sicherheitsempfindlichen Tätigkeit von der entscheidenden Stelle mit Auflagen

verbunden, muss die entscheidende Stelle auch die Tragung allfälliger Kosten der Auflagen regeln. Hierbei sind insbesondere allfällige arbeitsrechtliche oder vertragsrechtliche Vorschriften zu beachten. Die mangelnde Erfüllung allfälliger Auflagen sollte jedoch in letzter Konsequenz dazu führen, dass der geprüften Person die sicherheitsempfindliche Tätigkeit entzogen wird, da ohne die Auflagen das Sicherheitsrisiko nicht auf ein tragbares Mass reduziert werden kann.

Absatz 2: Die Mitteilung des Entscheids über die Ausübung der Tätigkeit ist für den Zutritt zu militärischen Anlagen oder zu Sicherheitszonen nötig. Sie ist auch für die Ausstellung einer Sicherheitsbescheinigung im internationalen Verhältnis nach Artikel 30 Absatz 2 Buchstabe b massgebend.

Art. 25 Mehrmalige Verwendung einer Erklärung

Absatz 1: Wenn für die betroffene Person bereits eine noch gültige und gleichwertige Erklärung ausgestellt wurde, soll in der Regel aus Gründen der Wirtschaftlichkeit keine neue Prüfung durchgeführt werden. Der Entscheid darüber im Einzelfall soll beim Risikoträger liegen.

Absatz 2: Wird für eine neue Prüfung die Erklärung einer früheren Prüfung verwendet, kann dies, wenn die frühere Prüfung in einer höheren Prüfstufe erfolgte, aus datenschutzrechtlicher Perspektive zur problematischen Situation führen, dass bei der höheren Prüfstufe erhobene Daten, die bei einer niedrigeren Prüfstufe nicht erhoben werden dürften, in die Beurteilung einfliessen. Die datenschutzrechtlich geforderte Ignorierung dieses Wissens kann im Einzelfall zu sicherheitspolitisch stossenden Ergebnissen führen. Es soll daher in Analogie zu den restriktiven Regelungen für die Verwertung von Zufallsfunden in anderen Rechtsgrundlagen eine klar beschränkte Verwertbarkeit möglich sein.

Art. 26 Ordentliche Wiederholung

Das ISG schreibt keine festen ordentlichen Wiederholungsintervalle vor. Es setzt diesbezüglich lediglich Leitplanken fest. Um auch hier die Prüfmenge angemessen steuern zu können, sollen, in Abhängigkeit zum Sicherheitsbedarf, klare Fristen für die Wiederholung festgelegt werden. Das ISG erteilt dem Bundesrat zudem die Kompetenz, bei Angehörigen der Armee oder des Zivilschutzes auf eine Wiederholung zu verzichten. Dies soll für die Fälle umgesetzt werden, bei denen eine Wiederholungsprüfung mit Blick auf die noch verbleibende Dienstzeit unverhältnismässig erscheint.

Art. 27 Ausserordentliche Wiederholung

Absatz 1: Für eine ausserordentliche Wiederholung dürfen nur neue Risiken massgebend sein, die für die Risikobeurteilung für die Ausübung der Tätigkeiten, wesentlich sind. Kein Grund für die Einleitung einer vorzeitigen Wiederholung sind hingegen Verstösse gegen die Anstellungsbedingungen. Für solche Verstösse sind personalrechtliche Massnahmen vorgesehen.

Absatz 2: Das ISG sieht eine ausserordentliche Wiederholung nur bei begründetem Verdacht auf neue Risiken vor. Für den Arbeitgeber kann aber auch der Wegfall von früher festgestellten Risiken von Bedeutung sein, da damit allfällige Einschränkungen bei der Ausübung von sicherheitsempfindlichen Tätigkeiten nicht mehr notwendig sind. Es soll daher auch in diesen Fällen eine ausserordentliche Wiederholung eingeleitet werden können.

Art. 28 Wirkung der Wiederholung

Die Wirkung der Wiederholung gilt sowohl für eine ordentliche wie auch eine ausserordentliche Wiederholung. Da die Wiederholung einer Neubeurteilung der zu prüfenden Person dient, soll bis zum Vorliegen der neuen Beurteilung die bisherige Beurteilung für die Ausübung der sicherheitsempfindlichen Tätigkeiten massgebend sein. Werden jedoch noch während der Wiederholungsprüfung neue Risiken erkannt, muss die entscheidende Stelle allenfalls mit angemessenen Massnahmen sorgen, dass sich diese Risiken bis zum Abschluss der Prüfung nicht verwirklichen können. Dies kann insbesondere durch den vorläufigen Entzug gewisser Tätigkeiten oder vorläufiger Änderungen des Pflichtenheftes erfolgen.

Art. 29 Rechtsschutz

Die Fachstellen PSP sind nach Artikel 31 Absatz 2 ISG in ihrer Beurteilung weisungsungebunden. Dies muss auch für die Führung von Beschwerdeverfahren zu den Beurteilungen gelten, damit die den Fachstellen PSP vorgesetzten Stellen nicht durch die Nichtgewährung der Beschwerdeführung indirekt auf die Beurteilungen Einfluss nehmen können. Die Fachstellen PSP müssen daher selber

entscheiden können, ob sie gegen Entscheide des Bundesverwaltungsgerichts Beschwerde führen wollen.

Art. 30 Sicherheitsbescheinigung im internationalen Verhältnis

Ausländische Sicherheitsbehörden gewähren ausschliesslich sicherheitsgeprüften Personen Zugang zu klassifizierten Informationen, klassifiziertem Material und Sicherheitszonen. Für die Ausstellung der sogenannten «personnel security clearance» ist das Verfahren festzulegen. Für die «clearance» massgebend ist der Entscheid der entscheidenden Stelle nach Artikel 24 und nicht das Ergebnis der Beurteilung durch die Fachstellen PSP. Soweit die «clearance» nicht im Interesse des Bundes erfolgt, soll eine Sicherheitsbescheinigung kostenpflichtig sein.

7. Abschnitt: Bearbeitung von Personendaten

Art. 31 Verantwortung für den Datenschutz und die Datensicherheit

In Anwendung von Artikel 16 Absatz 2 DSG muss die Organisation der Zuständigkeiten und Verantwortungen für den Datenschutz, der auch Datensicherheit verlangt, im Zusammenhang mit dem Informationssystem nach Artikel 45 ISG geregelt werden. Dabei soll der Grundsatz angewendet werden, dass der jeweilige Datenherr die Verantwortung trägt.

Art. 32 Periodische Kontrolle der Bearbeitung von Personendaten

Da die Daten, die im Rahmen der Prüfungen bearbeitet werden, besonders sensibel sind, soll die Rechtmässigkeit ihrer Bearbeitung periodisch durch eine Stelle kontrolliert werden, die von den im Prüfverfahren involvierten Stellen unabhängig ist.

8. Abschnitt: Schlussbestimmungen

Art. 33 Vollzug

Künftig soll der Geschäftsverkehr soweit wie möglich elektronisch stattfinden.

Art. 34 Gebührenerhebung

Die Kosten für die Prüfungen aus der zentralen Bundesverwaltung sollen zentral beim VBS budgetiert werden. Die Kosten für die Prüfungen für Stellen ausserhalb der zentralen Bundesverwaltung sollen dezentral von diesen getragen und mittels Gebühren beglichen werden. Der Bundesrat hat durch entsprechende Gewährung der finanziellen und personellen Ressourcen an das VBS dafür zu sorgen, dass zwischen diesen Ressourcen und der Anzahl durchzuführender Prüfungen jederzeit ein Gleichgewicht besteht.

Art. 35 Leistungen der Fachstellen PSP zugunsten der Kantone

Gemäss Artikel 86 Absatz 4 ISG können die Kantone gegen Gebühr die Leistungen der Fachstellen nach dem ISG für ihre eigene Informationssicherheit in Anspruch nehmen, soweit der Bundesrat dies festlegt. Durch Artikel 16 ist ersichtlich, dass die Fachstelle PSP VBS für Personensicherheitsprüfungen der Kantone zuständig ist. Für eine solche Inanspruchnahme müssen die Kantone über eine eigene rechtliche Grundlage für Prüfungen verfügen und die Fachstelle PSP VBS muss fachlich geeignet sein, die geforderten Beurteilungen vornehmen zu können. Da es sich dabei faktisch um gewerbliche Dienstleistungen des Bundes handelt, sollen die für gewerbliche Dienstleistungen des Bundes üblichen Voraussetzungen gelten, insbesondere das Prinzip der Kostendeckung. Das VBS schliesst mit den jeweiligen Kantonen eine Leistungsvereinbarung ab, damit das Mengengerüst der Prüfungen und damit der Aufwand für das VBS voraussehbar und planbar ist. Sollten die zu erbringenden Leistungen zusätzliche Mittel der Fachstellen erfordern, können die Leistungen nur erbracht werden, wenn den Fachstellen diese zusätzlichen Mittel auch tatsächlich gewährt werden. Eine bundesinterne Kompensation dieser Mittel ist ausgeschlossen.

Art. 36 Aufhebung anderer Erlasse

Um die Anzahl der Prüfungen in einem vernünftigen Rahmen zu behalten, müssen die Funktionenlisten konsequent erstellt und nachgeführt werden. Das VBS, das die Kosten der PSP trägt, wird deshalb die Funktionenlisten zentral bewirtschaften. Die Departemente und die BK beantragen als die eigentlichen Risikoträger laufend die notwendigen Änderungen der Funktionenlisten. Die entsprechenden heutigen Departementsverordnungen sind daher aufzuheben. Ebenso aufzuheben ist die geltende Verordnung über die Personensicherheitsprüfungen, die mit der vorliegenden Verordnung totalrevidiert wird. Ferner ist die Verordnung über die Personensicherheitsprüfungen

im Bereich Kernanlagen aufzuheben, da deren Inhalte, soweit noch erforderlich, in die vorliegende Verordnung integriert werden.

Art. 37 Änderung anderer Erlasse

Aufgrund des Umfangs der Änderung anderer Erlasse erfolgt die entsprechende Regelung im Anhang 9. Die Erläuterung dazu folgt weiter unten.

Art. 38 Übergangsbestimmungen

Die Erklärungen zu den heutigen Prüfungen kennen kein formelles Ablaufdatum, die Prüfung wird lediglich nach einer bestimmten Frist wiederholt. Die vorgeschlagene Regelung bietet sowohl den einleitenden Stellen als auch den Fachstellen PSP Kontinuität. Sie geben ferner genügend Spielraum, um zuerst die kritischsten Funktionen neu prüfen zu lassen. Für die Prüfungen nach StromVG, die bisher auf privatrechtlicher Basis erfolgten, bedarf es zudem einer speziellen Regelung, damit der bestehende Vertrag ordentlich beendet werden kann.

Art. 39 Inkrafttreten

Der Zeitpunkt des Inkrafttretens ist vorderhand eine angestrebte Zielgrösse. Für den effektiven Zeitpunkt sind unter anderem das weitere Rechtsetzungsverfahren und der zeitliche Bedarf für die technische Umsetzung der neuen Regelungen im Informationssystem PSP relevante Einflussgrössen.

Anhänge 1–6 Funktionenlisten

Die Anhänge 1, 4 und 6 werden zum Schutz der inneren und äusseren Sicherheit der Schweiz nicht veröffentlicht (siehe Erläuterung zu Art. 5).

Anhang 7 Datenerhebung

Anhang 7 enthält die detaillierte Datenerhebung und -bearbeitung für die Prüfungen. Die gesetzlichen Schranken, die das ISG für die Bearbeitung der Daten festlegt (Vgl. z. B. Art. 27 Abs. 3 oder Art. 34 Abs. 4 ISG), werden hier nicht wiederholt. Die Datenliste ist nicht abschliessend, wie der Begriff «insbesondere» zeigt. In beiden Ziffern handelt es sich um Kann-Vorschriften. Die Fachstellen müssen also nicht unbedingt auf alle verfügbaren Mittel zugreifen, um das Risiko zu beurteilen. So macht es beispielsweise wenig Sinn, Steuerdaten von Stellungspflichtigen zu erheben, da diese in ihrem jungen Alter noch gar keine oder keine aussagekräftigen Steuererklärungen eingereicht haben. Dies ist insbesondere bei der Prüfstufe erweiterte Personensicherheitsprüfung wichtig, weil die Reduktion der Prüfstufen nicht dazu führen soll, dass die Kosten der PSP unnötig massiv erhöht werden.

Zur Datenerhebung und -bearbeitung aus öffentlich zugänglichen Quellen (sog. Open Source Information, OSINF) kann festgehalten werden, dass es sich nie um private beziehungsweise vertrauliche Informationen handelt. Somit tangieren OSINF-Ermittlungen weder die von der Verfassung geschützte Privatsphäre noch das Fernmeldegeheimnis. Es handelt sich dabei auch nicht um eine geheime Überwachungsmassnahme. Mangels einer direkten Kontaktaufnahme seitens des Ermittlers mit der Zielperson liegt auch keine verdeckte Fahndung vor. OSINF-Ermittlungen sind eine legitime und aufgrund der fortschreitenden Digitalisierung an Bedeutung gewinnende Methode zur Beschaffung und Bearbeitung von Informationen.

Anhang 8 Änderung anderer Erlasse

1. OV-VBS

Die Fachstellen PSP sind gemäss Artikel 31 Absatz 2 ISG lediglich in ihrer Beurteilung weisungsungebunden. Sie gehören daher nach den Artikel 7 ff. RVOV zur zentralen Bundesverwaltung und können nicht administrativ zugeordnet werden. Die aufgrund des bisher anwendbaren Artikel 21 Absatz 1 BWIS in Artikel 6 Buchstabe c OV-VBS enthaltene administrative Zuordnung der Fachstelle PSP VBS ist daher aufzuheben.

2. BPV

Art. 94e Auszug aus dem Strafregister und dem Betreibungsregister

Die Möglichkeit des Arbeitgebers, einen Auszug aus dem Strafregister und dem Betreibungsregister zu verlangen, besteht nur dann, wenn der Arbeitgeber ein legitimes Interesse nach Absatz 1

hat. Mit dem Begriff «politisches Interesse» wird insbesondere den guten Ruf der Bundesverwaltung erfasst. Die Möglichkeit nach Artikel 94*e* BPV ist als jenes Mittel in der Kaskade der Sicherheitsüberprüfungen zu verstehen, welches am wenigsten stark in die Persönlichkeitsrechte der betroffenen Personen eingreift. Diese Bestimmung kommt grundsätzlich nur zur Anwendung, wenn die in Frage stehende Funktion nicht bereits von einer Prüfung nach der VPSP abgedeckt ist. Sie kann dennoch auch zur Anwendung kommen, wenn die PSP vor langer Zeit durchgeführt wurde und der Arbeitgeber einen begründeten Verdacht hat, dass ein Risiko besteht. Es darf aber kein Automatismus entstehen, wonach für Funktionen, die keiner anderen Prüfung unterstellt sind, systematisch Registerauszüge verlangt werden. Nur wenn eine Funktion aufgrund ihres Aufgabenbereiches klar die Voraussetzungen von Absatz 1 erfüllt, darf der Arbeitgeber Auszüge verlangen. Aus wichtigen Gründen, wie etwa ein konkreter Einsatz oder ein besonderer Auftrag, kann bereits früher als fünf Jahre ein neuer Auszug verlangt werden. Es ist in der Verantwortung des jeweiligen Arbeitgebers zu entscheiden, ob aufgrund eines Registereintrags ein Risiko besteht und gegebenenfalls, welche personalrechtlichen Massnahmen zu treffen sind.

Art. 94f Prüfung der Vertrauenswürdigkeit

Die Voraussetzungen einer Prüfung der Vertrauenswürdigkeit nach Artikel 20*b* BPG sollen in der BPV geregelt werden. Das Verfahren der Prüfung soll jedoch vollständig in der VPSP enthalten sein.

3. VIMK

Der bestehende Querverweis auf die bisher geltende PSPV ist an das neue Recht anzupassen.

4. Verordnung vom 16. Dezember 2009[33] über die militärischen Informationssysteme (MIV)

Mit der Regelung des Informationssystems Personensicherheitsprüfungen im ISG und der vorliegenden Verordnung sind die entsprechenden Artikel 67 und Anhang 30 der MIV aufzuheben. Zudem sind die bestehenden Querverweise auf die bisher geltende PSPV an das neue Recht anzupassen.

5. Verordnung vom 22. November 2017[34] über die Militärdienstpflicht

Die bestehenden Querverweise auf die bisher geltende PSPV sind an das neue Recht anzupassen.

6. Kernenergieverordnung vom 10. Dezember 2004[35] (KEV)

Aufgrund der Aufhebung der Verordnung über die Personensicherheitsprüfungen im Bereich der Kernanlagen beziehungsweise deren Integration in die VPSP soll in der KEV ein Querverweis auf die VPSP aufgenommen werden, damit der rechtsinteressierte Leser die entsprechenden Bestimmungen einfacher finden kann. Die Kostentragung soll hingegen in die KEV aufgenommen werden.

4.4 Verordnung über das Betriebssicherheitsverfahren (VBSV)

Einleitende Bemerkungen

Zum Verständnis der Materie erscheinen an dieser Stelle mindestens zu den nachfolgenden Bestimmungen des ISG kurze Ausführungen:

- Wenn von sicherheitsempfindlichen Aufträgen die Rede ist, so ist hierbei auf die Legaldefinitionen von Artikel 5 Buchstabe b ISG abzustützen. Demnach beinhalten solche Aufträge die Bearbeitung von VERTRAULICH oder GEHEIM klassifizierten Informationen gemäss Artikel 13 ISG, die Verwaltung, den Betrieb und die Überprüfung von Informatikmitteln der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz» gemäss Artikel 17 ISG sowie den Zugang zu Sicherheitszonen, einschliesslich zu Schutzzonen nach der Gesetzgebung über den Schutz militärischer Anlagen. Die Rechtsform der Aufträge ist unerheblich.
- Als Betriebe im Sinne der VBSV gelten Unternehmen oder Subunternehmen oder Teile davon, die einen öffentlichen Auftrag erfüllen, welcher eine sicherheitsempfindliche Tätigkeit einschliesst (vgl. Art. 49 ISG).
- Als Auftraggeberinnen im Sinne der VBSV walten die verpflichteten Behörden oder Organisationen nach Artikel 2 ISG (vgl. Art. 50 Abs. 1 Bst. a ISG).

[33] SR **510.911**
[34] SR **512.21**
[35] SR **732.11**

Ingress

Das Betriebssicherheitsverfahren bildet innerhalb des 4. Kapitels des ISG einen in sich geschlossenen Normenkomplex, welcher die Grundlage für die entsprechende Ausführungsgesetzgebung bildet. Artikel 84 Absatz 1 ISG enthält die grundsätzliche Kompetenz der verpflichteten Behörden zum Erlass von Ausführungsbestimmungen zum ISG Artikel 73 weist dem Bundesrat konkret die im Einzelnen zu regelnden Bereiche zu.

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Gegenstand und Geltungsbereich

Absatz 1: Die Bestimmung lehnt sich für den Beschrieb der Regelungsmaterie der VBSV an die in Artikel 73 ISG dem Bundesrat auferlegten Rechtsetzungsaufträge an.

Absatz 2: Soweit Behörden und Organisationen dem Geltungsbereich des ISG beziehungsweise der ISV unterliegen, kommen sie auch als Auftraggeberinnen von sicherheitsempfindlichen Aufträgen in Frage. Der Geltungsbereich der VBSV muss somit deckungsgleich mit jenem von ISG und ISV sein (vgl. auch Ziff. 3.6 Bst. a).

Art. 2 Betroffene Betriebe

Absatz 1: Den Grundtatbestand für die Durchführung des Betriebssicherheitsverfahrens bildet die Vergabe von sicherheitsempfindlichen Aufträgen durch schweizerische Behörden und Organisationen an Betriebe mit Sitz in der Schweiz. Subunternehmen mit Sitz in der Schweiz werden diesen Betrieben gleichgestellt. Der Begriff des Betriebes ist in einem weiten Sinne zu verstehen. So spielen weder Rechtsform noch Grösse eine Rolle. Entscheidend sind einzig die Sicherheitsempfindlichkeit des Auftrages und die Unterstellung des Betriebes unter die schweizerische Rechtsordnung.

Dezentralisierte Verwaltungseinheiten der Bundesverwaltung sowie Organisationen und Personen des öffentlichen und privaten Rechts, die mit Bundesaufgaben betraut werden, können ebenfalls als Betriebe gelten, sofern sie nicht dem Geltungsbereich des ISG unterstellt sind.

Absatz 2: Die VBSV umfasst die nationalen Sachverhalte. Die Durchführung von Betriebssicherheitsverfahren für Betriebe mit Sitz im Ausland richtet sich nach den entsprechenden völkerrechtlichen Verträgen.

Art. 3 Zuständige Behörde

Absatz 1: Die Behörde «Fachstelle Betriebssicherheit» (Fachstelle BS) muss organisatorisch zugewiesen werden. Der entsprechende Entscheid wird zusammen mit dem Entscheid über die administrative Zuordnung der Fachstelle des Bundes für Informationssicherheit getroffen (vgl. Ziff. 3.8).

Absatz 2: Im Zusammenhang mit grenzüberschreitenden Betriebssicherheitsverfahren ist die Fachstelle BS auf die Zusammenarbeit mit der designierten schweizerischen Sicherheitsbehörde angewiesen, über welche die Auslandkontakte ausschliesslich laufen. Die Abstimmung des Betriebssicherheitsverfahrens mit den Verfahrensabläufen der designierten schweizerischen Sicherheitsbehörde obliegt der Fachstelle BS.

2. Abschnitt: Einleitung des Betriebssicherheitsverfahrens

Einleitende Bemerkung zum zweiten Abschnitt

Die Einleitung des Verfahrens soll zu einem möglichst frühen Zeitpunkt im Beschaffungsprozess erfolgen können. In dieser ersten Phase soll vor allem abgeklärt werden, ob der zu vergebende Auftrag sicherheitsempfindlich ist und somit die zentrale Prozessvoraussetzung gegeben ist. Es werden keine Präjudize für das Vergabeverfahren geschaffen.

Art. 4 Antrag auf Einleitung des Verfahrens

Absatz 1 Buchstaben a und b: Die Informationssicherheitsbeauftragten bieten die Gewähr, dass Informationssicherheitsaspekte frühzeitig in die Überlegungen einer Vergabe an Dritte einfliessen.

Absatz 1 Buchstabe c: Betriebe, die einen Unterauftrag vergeben, begeben sich damit ihrerseits in die Rolle einer Auftraggeberin. Sofern sie von ihrer eigenen Auftraggeberin überhaupt zur Vergabe eines Unterauftrages ermächtigt werden, soll es ihnen folglich auch obliegen, den Antrag auf Einleitung des Betriebssicherheitsverfahrens zu stellen. Zuständig ist die oder der Betriebssicherheitsbeauftragte nach Artikel 12.

Absatz 2: Bei den verpflichteten Behörden nach Artikel 2 Absatz 1 ISG kommt dem Bundesrat (ausser bei sich selber) keine Kompetenz zu, die Zuständigkeit für die Einleitung des Verfahrens festzulegen. Er beschränkt sich daher in der VBSV darauf, die verpflichteten Behörden die zuständige Stelle melden zu lassen.

Absatz 3 Buchstabe a: Die Umschreibung der Bauleistung, Lieferung oder Dienstleistung dient der Fachstelle BS insbesondere als Identifizierungsmerkmal, insbesondere dann, wenn ein Betrieb mehrere sicherheitsempfindliche Aufträge ausführt.

Absatz 3 Buchstabe b: Da die Sicherheitsempfindlichkeit des Auftrages Eintretensvoraussetzung für das Betriebssicherheitsverfahren ist, muss mindestens mit summarischer Begründung dargelegt werden, inwiefern die Voraussetzungen nach Artikel 5 Buchstabe b ISG gegeben sind. Die Beweiserleichterung durch eine nur summarische Begründung soll insbesondere dazu dienen, dass eine Einleitung des Verfahrens zu einem relativ frühen Zeitpunkt stattfinden kann mit dem Ziel, die Verfahrensabläufe des Vergabeverfahrens möglichst wenig zu tangieren.

Absatz 3 Buchstabe c: Das Betriebssicherheitsverfahren ist im Einzelfall frühzeitig auf die Verfahrensbestimmungen im öffentlichen Beschaffungswesen abzustimmen. Es ist der Verfahrensökonomie daher zuträglich, wenn die Auftraggeberin bereits in diesem frühen Stadium klare Vorstellungen über das anwendbare Vergabeverfahren hat.

Art. 5 Prüfung des Antrags

Absatz 1: Der Fachstelle BS kommt hinsichtlich der Einleitung des Verfahrens ein relativ erheblicher Ermessensspielraum zu, welchen sie jedoch stets im Einvernehmen mit der in- oder ausländischen Auftraggeberin auszuüben hat (vgl. Art. 53 Abs. 2 ISG).

Absatz 2: Mit dieser Bestimmung schränkt der Bundesrat den Ermessensspielraum der Fachstelle BS ein und setzt abschliessend die Sachverhalte fest, bei denen das Betriebssicherheitsverfahren zwingend einzuleiten ist. Es sind dies die folgenden vier Konstellationen:

- Buchstabe a: Betriebe, welche im Bereich des höchsten Schutzbedarfs von Informationen und Informatikmitteln arbeiten, sollen ungeachtet der Art oder des Ortes der Auftragserfüllung immer unter die Bestimmungen der VBSV fallen.
- Buchstabe b: Der Bundesrat bestimmt hier, dass die Bearbeitung VERTRAULICH klassifizierter Informationen, bei denen das Geheimhaltungsinteresse auf mehrere Behörden oder Departemente verteilt ist, ausnahmslos ein Fall für das Betriebssicherheitsverfahren ist.
- Buchstabe c: Analog zu Buchstabe b sollen auch der Betrieb, die Wartung oder die Überprüfung von Informatikmitteln der Sicherheitsstufe «hoher Schutz», wenn sie behörden- oder departementsübergreifend eingesetzt werden, ausnahmslos das Betriebssicherheitsverfahren auslösen.
- Buchstabe d: Eine internationale Betriebssicherheitsbescheinigung muss über eine solide Grundlage verfügen, für welche einzig die Durchführung des Betriebssicherheitsverfahrens nach ISG die notwendige und hinreichende Gewähr bietet. Der Betrieb kann jedoch, obwohl er für die Kosten des Verfahrens aufzukommen hat, nicht einfach auf diese Weise ein staatliches Gütesiegel «kaufen». Die Fachstelle BS wird auf das Verfahren nur eintreten, wenn ein entsprechender Antrag einer ausländischen Behörde oder internationalen Organisation vorliegt und es sich tatsächlich um einen sicherheitsempfindlichen Auftrag handelt.

Absatz 3: Diese Ordnungsfrist soll den Auftraggeberinnen einen Anhaltspunkt für die Planung und Koordination des Vergabeverfahrens geben und die Fachstelle BS zur Beachtung des Beschleunigungsgebotes anhalten.

Art. 6 Prüfung des Antrages mit ausländischen Sicherheitsbehörden

Absatz 1: Beabsichtigt die Auftraggeberin einen ausländischen und somit nicht der schweizerischen Rechtsordnung unterliegenden Betrieb mit einem sicherheitsempfindlichen Auftrag (vgl. Art. 49 ISG) zu betrauen, reicht sie den entsprechenden Antrag gleichermassen bei der Fachstelle BS ein. Die notwendigen Verfahrensschritte erfolgen nun über die Fachstelle des Bundes für Informationssicherheit (vgl. Artikel 83 ISG) mit der ausländischen Sicherheitsbehörde.

Absatz 2: Soweit ein entsprechender völkerrechtlicher Vertrag (vgl. Art. 87 ISG) vorliegt, wird die ausländische Sicherheitsbehörde auf Antrag der Fachstelle des Bundes für Informationssicherheit entweder bestätigen, dass der Betrieb über eine Betriebssicherheitserklärung verfügt, oder das Betriebssicherheitsverfahren einleiten. Das Verfahren unterliegt vollumfänglich dem Recht des

Sitzstaates des Betriebes, eine entsprechende Betriebssicherheitserklärung erfolgt ebenfalls nach ausländischem Recht.

Art. 7 Festlegung der Sicherheitsanforderungen

Absatz 1: Mit der ISV und der VPSP werden die beiden massgebenden Erlasse genannt, welche bei der Festlegung der Sicherheitsanforderungen im Einzelfall zu berücksichtigen sind.

Absatz 2: Im internationalen Verhältnis geniesst der völkerrechtliche Vertrag Vorrang gegenüber der ISV und der VPSP.

Absatz 3: Die Auftraggeberin und die Fachstelle BS können vorbehältlich Artikel 6 Absatz 2 über die Einleitung des Verfahrens eine Einigung treffen. Ebenso soll es, nach erfolgter Einleitung des Verfahrens, möglich sein, dass sich die beiden Stellen über eine Aufgabenteilung sowohl im Vergabeverfahren als auch bei der Auftragserfüllung einigen. Dieses Vorgehen dürfte vor allem dort sinnvoll sein, wo nach Erteilung der Betriebssicherheitserklärung für deren Dauer umfangreiche oder dauernde Kontrollmassnahmen angezeigt sind. Es liegt dort im direkten Interesse der Auftraggeberin (Geheimnisherrin), unabhängig von der Fachstelle BS Kontrollen durchführen zu können. Nicht an die Auftraggeberin übertragbar sind behördliche Zwangsmassnahmen.

Absatz 4: Im Verhältnis zwischen dem Vergabeverfahren und dem Betriebssicherheitsverfahren bildet stets das Vergabeverfahren das Leitverfahren. Das Betriebssicherheitsverfahren folgt als Instrument der Informationssicherheit stets den Abläufen des Vergabeverfahrens. Bei letzterem sind jedoch die Schritte des Betriebssicherheitsverfahrens in den Verfahrensplan zu integrieren. Die entsprechenden Koordinationsaufgaben obliegen konsequenterweise der hauptinteressierten Partei im Leitverfahren, der Auftraggeberin.

3. Abschnitt: Beurteilung der Betriebe

Art. 8 Durchführung der Eignungsprüfung

Absatz 1: Mit der Eignungsprüfung nimmt die Fachstelle BS im Gegensatz zur Prüfung über die blosse Einleitung des Verfahrens nunmehr ungleich aufwändigere und tiefgreifendere Amtshandlungen an die Hand. Aus rechtlichen und verfahrensökonomischen Gründen ist es in diesem Stadium des Betriebssicherheitsverfahrens daher unerlässlich, dass diesen Untersuchungen nur noch Betriebe unterzogen werden, welche aus Sicht der Auftraggeberin für den Zuschlag noch in Frage kommen. Grundsätzlich sollen der Fachstelle BS nicht mehr als fünf Betriebe zur Eignungsprüfung gemeldet werden. Eine Erweiterung soll nur in begründeten Fällen stattfinden können. Diese Ausnahmeklausel soll insbesondere einen Ausweg für unvorhergesehene Entwicklungen im Vergabeverfahren bilden und Nachmeldungen ermöglichen.

Absatz 2: Die Einwilligung des Betriebes in die Durchführung des Verfahrens ist Eintretensvoraussetzung (vgl. Art. 50 Abs. 2 ISG) und daher von der Fachstelle BS von Amtes wegen zu prüfen. Diese Einwilligung kann eine explizite sein oder sich bereits aus den in den Ausschreibungsunterlagen aufgestellten und vom Betrieb akzeptierten Teilnahmebedingungen ergeben.

Absatz 3 Buchstabe a: Gemäss Artikel 56 Absatz 1 Buchstabe a ISG kann die Fachstelle BS zur Beurteilung der Eignung der Betriebe bei diesen selber entsprechende Daten erheben. Den Betrieben obliegt hiermit eine Mitwirkungspflicht, welche in Artikel 9 Buchstaben a–g umrissen wird. Legt ein Betrieb eine mangelhafte Mitwirkungsbereitschaft an den Tag, ist dies mit einer Nichteinwilligung ins Verfahren gleichzusetzen. Das Verfahren wird aufgrund einer fehlenden Prozessvoraussetzung für den entsprechenden Betrieb eingestellt.

Absatz 3 Buchstabe b: Falsche Angaben stellen im Gegensatz zu verweigerten Angaben (Bst. a) zwar kein Prozesshindernis dar, sind aber in den Erwägungen zum Entscheid über die Vertrauenswürdigkeit zu berücksichtigen und führen in der Regel dazu, dass der Betrieb als Sicherheitsrisiko beurteilt wird.

Absatz 4: Diese Ordnungsfrist soll analog zu Artikel 5 Absatz 3 den Auftraggeberinnen einen Anhaltspunkt für die Planung und Koordination des Vergabeverfahrens geben und die Fachstelle BS zur Beachtung des Beschleunigungsgebotes anhalten.

Art. 9 Datenerhebung

Absatz 1 Buchstaben a–g: Diese Bestimmungen konkretisieren Artikel 56 ISG und führen in einer nicht abschliessenden Aufzählung die Punkte auf, welche als geeignet erachtet werden, den Betrieb hinsichtlich seiner Vertrauenswürdigkeit sowie seiner Beziehungen zu ausländischen Staaten

und Organisationen sicherheitsmässig beurteilen zu können. Die Erhebungen werden von der Fachstelle BS durchgeführt.

Absatz 2: Die Erhebung der Daten nach Artikel 6 Absatz 1 Buchstabe a des Nachrichtendienstgesetzes vom 25. September 2015[36] (NDG) fällt in die Zuständigkeit des NDB. Hierbei wird untersucht, ob der Betrieb bisher in Zusammenhang mit Terrorismus, verbotenem Nachrichtendienst, Proliferation, Angriffen auf kritische Infrastrukturen oder gewalttätigem Extremismus in Erscheinung getreten ist. Die Erhebungen werden durch den NDB durchgeführt.

Absatz 3 Buchstabe a: Gemäss Artikel 56 Absatz 1 Buchstabe a ISG kann die Fachstelle BS zur Beurteilung der Eignung der Betriebe bei diesen selber entsprechende Daten erheben. Den Betrieben obliegt hiermit eine Mitwirkungspflicht, welche in Artikel 9 Absatz 1 Buchstaben a–g umrissen wird. Legt ein Betrieb eine mangelhafte Mitwirkungsbereitschaft an den Tag, ist dies mit einer Nichteinwilligung ins Verfahren gleichzusetzen. Das Verfahren wird aufgrund einer fehlenden Prozessvoraussetzung für den entsprechenden Betrieb eingestellt.

Absatz 3 Buchstabe b: Falsche Angaben stellen im Gegensatz zu verweigerten Angaben (Bst. a) zwar kein Prozesshindernis dar, sind aber in den Erwägungen zum Entscheid über die Vertrauenswürdigkeit zu berücksichtigen und führen in der Regel dazu, dass der Betrieb als Sicherheitsrisiko beurteilt wird.

Art. 10 Ausschluss vom Verfahren

Absatz 1: Sowohl Artikel 44 des Bundesgesetzes über das öffentliche Beschaffungswesen vom 21. Juni 2019[37] (BöB) als auch Artikel 57 ISG zählen diverse Sachverhalte auf, bei deren Vorliegen die Auftraggeberin einen Betrieb vom Vergabeverfahren ausschliessen kann oder muss. Damit Vergabe- und Betriebssicherheitsverfahren einander nicht unnötig blockieren, soll die Tatsache, dass erste Anhaltspunkte für das Vorhandensein von Ausschlussgründen nach Artikel 44 BöB vorliegen, die Aufraggeberin nicht davon abhalten, der Fachstelle BS einen solchen Betrieb zur Durchführung der Eignungsprüfung zu melden, ohne dass sie bereits über einen Ausschluss entscheiden muss. Sie soll ihre entsprechenden Erkenntnisse jedoch der Fachstelle BS zum Zweck der Eignungsprüfung mitteilen. Andererseits soll die Fachstelle BS die Auftraggeberin auch schnellstmöglich informieren, wenn aufgrund ihrer Datenerhebung Erkenntnisse zu Tage treten, welche die Auftraggeberin dazu anhalten können, den Betrieb auszuschliessen.

Absatz 2: Aufgrund dieses laufenden Informationsaustausches ist es gerechtfertigt, dass die Fachstelle BS einen zweifelhaften Betrieb vorerst weiter auf seine Eignung prüft, bis die Auftraggeberin über einen allfälligen Ausschluss entschieden hat.

Absatz 3: Wenn im Vergabeverfahren bereits ein Ausschluss durch die Auftraggeberin erfolgt, fehlt dem Betriebssicherheitsverfahren der Verfahrensgegenstand. Somit liegt ein klarer Fall von Artikel 51 Absatz 1 Buchstabe c ISG vor und das Betriebssicherheitsverfahren ist für den betreffenden Betrieb ohne Weiteres einzustellen.

Art. 11 Informationsaustausch

Diese Bestimmung äussert sich über den Inhalt des gegenseitigen Informationsaustausches. So sollen der Fachstelle BS für Eignungsprüfung einerseits sachdienliche Hinweise vergaberechtlicher Natur und der Auftraggeberin andererseits sicherheitsrelevante Erkenntnisse für ihren Ausschlussentscheid nach Artikel 44 BöB zur Verfügung gestellt werden.

4. Abschnitt: Sicherheitskonzept

Art. 12 Betriebssicherheitsbeauftragte

Absatz 1: Ein Betrieb, welcher von der Auftraggeberin zur Eignungsprüfung angemeldet wird, soll eine Betriebssicherheitsbeauftragte oder ein Betriebssicherheitsbeauftragter bezeichnen und der Fachstelle BS melden. Damit die festgelegten Sicherheitsanforderungen auch die nötige Wirkung erzielen können, ist es notwendig, dass die Führung des Betriebs diesbezüglich in die Verantwortung genommen werden kann. Die Betriebssicherheitsbeauftragten müssen demnach innerhalb des Betriebes mindestens im Sicherheitsbereich über gewisse Weisungsrechte verfügen. Idealerweise sind sie selber Mitglied der Geschäftsleitung und können so auf die Entscheide einwirken oder sie handeln mindestens in direktem Auftrag einer solchen Person.

[36] SR **121**
[37] SR **172.056.1**

Absatz 2 Buchstabe a: Für eine effiziente und effektive Einflussnahme auf die Informationssicherheit des Betriebes braucht die Fachstelle BS eine Ansprechperson, über die alle Kontakte laufen können.

Absatz 2 Buchstabe b: Der oder die Sicherheitsbeauftragte ist gegenüber der Fachstelle BS bezüglich der Umsetzung des Sicherheitskonzepts Rechenschaft schuldig. Die Fachstelle BS sorgt für eine angemessene Aus- und Weiterbildung der Betriebssicherheitsbeauftragten.

Absatz 2 Buchstabe c: In den Fällen, da der Betrieb von der Auftraggeberin ermächtigt wurde, Subunternehmen beizuziehen, ist die oder der Betriebssicherheitsbeauftragte legitimiert, bei der Fachstelle BS den Antrag auf Einleitung des Betriebssicherheitsverfahrens für das Subunternehmen einzureichen (vgl. Art. 4 Abs. 1 Bst. c).

Art. 13 Mitteilung des Zuschlags

Absatz 1: Rahmenverträge dürften in der Regel das auslösende Element für den Erlass einer Betriebssicherheitserklärung sein. Hingegen können die mit dem Rahmenvertrag verbundenen Einzelauftragsverhältnisse unter Umständen das Risiko für die Informationssicherheit so beeinflussen, dass das Sicherheitskonzept angepasst werden muss. Es ist daher entscheidend, dass die Fachstelle BS über die sicherheitsempfindliche Auftragslage beim Betrieb immer auf dem Laufenden ist.

Absatz 2: Die für die Erstellung des Sicherheitskonzepts notwendigen, durch die Auftraggeberin zu liefernden Angaben umfassen insbesondere:

- Angaben über die Stufe der Sicherheitsempfindlichkeit des Auftrages nach Massgabe von Artikel 5 ISG;
- die Nennung der Personen, die mit der Ausführung des sicherheitsempfindlichen Auftrages betraut werden (zur Durchführung von Personensicherheitsprüfungen);
- Angaben über den Einsatz von betrieblichen Informatikmitteln, insbesondere, ob diese vernetzt betrieben oder vom Netz abgeschottet werden.

Art. 14 Inhalt und Prüfung des Sicherheitskonzepts

Absatz 1: Der Augenschein stellt sicher, dass dem Betrieb mit dem Sicherheitskonzept gezielt die notwendigen, geeigneten und der Gesamtsituation angepassten Massnahmen auferlegt werden können. Er dient damit einerseits der Informationssicherheit, schützt andererseits den Betrieb aber auch vor unverhältnismässigem Aufwand.

Absatz 2: Die Fachstelle BS gibt dem Betrieb für die Erstellung des Sicherheitskonzepts einen Rahmen vor, in welchem dieser nun die der Gesamtsituation angepassten Sicherheitsmassnahmen zu treffen und zu dokumentieren hat. Zu dokumentieren sind organisatorische (z.B. Schlüsselhandling, Raumüberwachung), personelle (Personensicherheitsprüfungen), technische (z.B. Einsatz von Informatikmitteln) und physische Massnahmen (Einbruchsicherungen).

Absatz 3: Die Erstellung von Sicherheitskonzepten kann sich als komplex erweisen, insbesondere da dem Betrieb bewusst auch gewisse Ermessensspielräume gewährt werden. Besteht das eingereichte Sicherheitskonzept die Prüfung durch die Fachstelle BS (vgl. Art. 59 Abs. 2 ISG) nicht auf Anhieb, so hat diese dem Betrieb eine Nachfrist zur Verbesserung zu gewähren und soll dabei auch konkrete Anweisungen erteilen, was und wie nachzubessern ist.

Absatz 4: Diese Ordnungsfrist soll analog zu Artikel 5 Absatz 3 den Auftraggeberinnen einen Anhaltspunkt für die Planung und Koordination des Vergabeverfahrens geben und die Fachstelle BS zur Beachtung des Beschleunigungsgebotes anhalten.

Art. 15 Personensicherheitsprüfungen

Absatz 1: Der Betrieb hat sich für die Ausführung eines sicherheitsempfindlichen Auftrags so zu organisieren, dass nur eine minimale, für die Erfüllung des Auftrages zwingend notwendige Anzahl von Personen einer PSP unterzogen werden muss. Prüfungsanträge für Personen, welche nur potenziell sicherheitsempfindliche Tätigkeiten ausüben, sind widerrechtlich und werden von der Fachstelle BS zurückgewiesen.

Absatz 2: Aus verfahrensökonomischen Gründen kann es Sinn machen, dass vor allem grosse Betriebe ermächtigt werden, PSP selbständig einzuleiten. Das ändert nichts daran, dass die Fachstelle BS abschliessend festlegt, welche Personen dann auch wirklich geprüft werden.

5. Abschnitt: Betriebssicherheitserklärung und Wiederholung des Verfahrens

Art. 16 Ausstellung der Betriebssicherheitserklärung

Im Gesetz nicht vorgesehen, jedoch als mit den Zielen des ISG vereinbar, wenn nicht gar durch das Verhältnismässigkeitsprinzip geboten, erscheint die Beschränkung der Betriebssicherheitserklärung auf einzelne Elemente von sicherheitsempfindlichen Tätigkeiten im Sinne von Artikel 5 Buchstabe b ISG. Es leuchtet einerseits ein, dass z.B. für die Bearbeitung von VERTRAULICH klassifizierten Informationen einem Betrieb nicht derart aufwändige Schutzmassnahmen auferlegt werden, welche für die Bearbeitung GEHEIM klassifizierter Informationen nötig sind. Andererseits soll ein auf VERTRAULICH ausgerichtetes Sicherheitskonzept zwingend angepasst werden müssen, wenn neu auch GEHEIM klassifizierte Informationen betroffen sind. Über die zugelassene Bearbeitungsstufe soll mittels Verfügung Rechtssicherheit hergestellt werden.

Art. 17 Meldungen des Betriebs

Absätze 1 und 2: Diese nicht abschliessende Aufzählung konkretisiert Artikel 63 Absatz 2 ISG hinsichtlich des Inhalts der Meldepflicht betreffend sicherheitsrelevanten Änderungen im Betrieb.

Absatz 3: Ein rechtzeitiges Eingreifen kann dadurch begünstigt werden, dass bereits bei einem Anfangsverdacht gehandelt wird und nicht erst die Auswirkungen eines Vorfalles abgewartet werden. Deshalb wird bereits der Verdacht auf einen Vorfall als meldepflichtig erklärt.

Absatz 4: Änderungen und Vorfälle können neben dem Betrieb auch Subunternehmen oder Lieferanten des Betriebs betreffen. Während die zugelassenen Subunternehmen selbständig der primären Meldepflicht nach den Absätzen 1 und 2 unterliegen, ist das für Lieferanten, welche nur mittelbar mit der sicherheitsempfindlichen Tätigkeit in Berührung kommen, nicht der Fall. Sofern diese von einem Vorfall betroffen sind, der auf die sicherheitsempfindliche Tätigkeit Auswirkungen haben kann, soll dies ebenfalls durch den Betrieb gemeldet werden.

Absatz 5: Mit dieser Bestimmung soll verhindert werden, dass die Gültigkeit einer Betriebssicherheitserklärung während eines laufenden Auftrages ausläuft und dadurch das Auftragsverhältnis auf einen Schlag in die Rechtswidrigkeit versetzt wird und grundsätzlich vollständig rückabzuwickeln wäre. Mit der rechtzeitigen Einleitung einer Erneuerung der Betriebssicherheitserklärung kann diese Situation umgangen werden (vgl. auch Ausführungen zu Art. 20 Abs. 2).

Art. 18 Pflichten der Auftraggeberin

Absatz 1: Die Auftraggeberinnen stehen mit den Betrieben naturgemäss häufig und eng in Kontakt, weshalb die Wahrscheinlichkeit auch gross ist, dass ihnen allfällige Missstände auffallen. Deshalb wird einerseits die Meldepflicht des Betriebes für sicherheitsrelevante Änderungen oder Vorfälle auf die Auftraggeberin ausgeweitet, soweit sie entsprechende Feststellungen beim Betrieb macht. Andererseits obliegt der Auftraggeberin zusätzlich auch das Treffen von Sofortmassnahmen.

Absatz 2 Buchstabe a: Sachverhalte nach Artikel 44 BöB können negative Auswirkungen auf die Umsetzung des Sicherheitskonzepts haben und sind daher unter Umständen auch im Lichte der Informationssicherheit zu würdigen. Die Auftraggeberin trifft daher eine Meldepflicht an die Fachstelle BS, wenn sie entsprechende Feststellungen macht. Diese Meldepflicht besteht auch dann, wenn die Auftraggeberin nicht beabsichtigt, den Zuschlag zu widerrufen.

Absatz 2 Buchstabe b: Sicherheitsrelevante Änderungen des Auftrages haben häufig Auswirkungen auf das Sicherheitskonzept, weshalb die Fachstelle BS auf dem Laufenden gehalten werden muss.

Absatz 2 Buchstabe c: Was für die Änderung eines Auftrages gilt, gilt sinngemäss auch für die Erteilung eines neuen Auftrages. Es wird auf die vorstehenden Ausführungen zu Buchstabe b verwiesen.

Art. 19 Internationale Betriebssicherheitserklärung

Absatz 1: Die Ausstellung einer internationalen Betriebssicherheitsbescheinigung stellt einen Verwaltungsakt ohne nennenswerte Besonderheiten und Aufwände dar, weshalb dafür eine Pauschalgebühr von 100 Franken erhoben wird.

Absatz 2: Anders sieht es aus, wenn der Betrieb noch über keine schweizerische Betriebssicherheitserklärung verfügt. Die vorgängig nötige Durchführung des Betriebssicherheitsverfahrens stellt einen Aufwand dar, welcher nach Zeitaufwand in Rechnung gestellt werden muss. Die Bandbreite des Stundenansatzes variiert je nach Dringlichkeit und der notwendigen Qualifikation des ausführenden Personals.

Absatz 3: Die Ausstellung einer internationalen Betriebssicherheitsbescheinigung ist grundsätzlich ein Verwaltungsakt zwischen der Fachstelle BS und dem Betrieb. Häufig wird sich jedoch die ausländische Sicherheitsbehörde an ihr schweizerisches Gegenüber wenden, um die Gültigkeit der ihr vorgelegten Bescheinigungen prüfen zu lassen. Es macht daher Sinn, wenn die Fachstelle BS der ausländischen Sicherheitsbehörde über die Fachstelle des Bundes für Informationssicherheit den Erlass einer internationalen Betriebssicherheitsbescheinigung auf Anfrage hin mitteilt oder mitteilen lässt.

Art. 20 Widerruf der Betriebssicherheitserklärung und Rückzug des Auftrags

Absatz 1: Soweit die Informationssicherheit nicht akut in Gefahr ist, soll dem Verhältnismässigkeitsprinzip folgend dem Betrieb vorerst die Möglichkeit eingeräumt werden, festgestellte Missstände zu korrigieren. Da die Auftraggeberin in diesem Verfahren ausnahmsweise die Rechte einer beschwerdeberechtigten Partei geniesst, ist sie vor dem Erlass von Verfahrensentscheiden jeweils anzuhören.

Absatz 2: In den seltenen Fällen eines Widerrufs der Betriebssicherheitserklärung ist zu beachten, dass damit zwei weitere, rechtlich bestreitbare Umstände ausgelöst werden. Einerseits hat die Auftraggeberin den Zuschlag (Verfügung) zu widerrufen und andererseits folgt die Auflösung eines privatrechtlichen Vertrages. Zur Sicherstellung der Informationssicherheit wird die Fachstelle BS einer Beschwerde gegen den Widerruf einer Betriebssicherheitserklärung in aller Regel vorsorglich gestützt auf Artikel 55 Absatz 2 des Verwaltungsverfahrensgesetzes vom 20. Dezember 1968[38] die aufschiebende Wirkung entziehen. Die Verfügung kann somit zeitverzugslos vollstreckt werden. Soweit die Auftraggeberin nicht die Ausnahmeklausel von Artikel 58 Absatz 3 ISG anruft, hat sie nun den sicherheitsempfindlichen Auftrag zurückzuziehen und sicherzustellen, dass dem Betrieb umgehend alle Möglichkeiten entzogen werden, die Informationssicherheit negativ zu beeinflussen. Wird der Widerruf der Betriebssicherheitserklärung angefochten, so wird dies auch für den Widerruf des Zuschlages zutreffen. Es ist davon auszugehen, dass die beiden Rechtsmittelverfahren vom Bundesverwaltungsgericht vereint werden. Auf Antrag einer Partei können im gleichen Verfahren auch die zivilrechtlichen Ansprüche beurteilt werden (vgl. Art. 40 Abs. 1 des Verwaltungsgerichtsgesetzes vom 17. Juni 2005[39]).

Absatz 3: Diese Ordnungsfrist soll es der Fachstelle BS erlauben, innert nützlicher Frist Klarheit über die Beseitigung einer Sicherheitsgefährdung zu erlangen und zu entscheiden, ob allenfalls ihr eigenes, hoheitliches Eingreifen noch nötig ist.

Art. 21 Wiederholung des Verfahrens

Absatz 1: Die vorliegende Bestimmung weist der Fachstelle BS die Zuständigkeit für die Einleitung des Wiederholungsverfahrens zu. Sie wird von Amtes wegen tätig. Im Gegensatz zum vereinfachten Verfahren (vgl. Art. 65 ISG) wird in diesem Fall das ganze Verfahren (inkl. Eignungsprüfung) durchgeführt.

Absatz 2: Diese Bestimmung soll verhindern, dass hängige Aufträge abgebrochen und rückabgewickelt werden müssen, wenn das Wiederholungsverfahren das Ablaufdatum der Betriebssicherheitserklärung überdauert. Der aktenkundige formelle Akt der Verfahrenseröffnung durch die Fachstelle BS soll genügen, um die Gültigkeitsdauer der auslaufenden Betriebssicherheitserklärung bis zum neuen Entscheid zu verlängern.

Absatz 3: Im Zuge des Wiederholungsverfahrens kann die Fachstelle BS zum Schluss kommen, dass die Voraussetzungen für eine Erneuerung der Betriebssicherheitserklärung nicht vorliegen oder das Verfahren aus anderen Gründen einzustellen ist. Dies alles sind Entscheide, welche der verlängerten Gültigkeitsdauer nach Absatz 2 ein Ende setzen. Die Rückabwicklung der Rechtsverhältnisse folgt den Regeln beim Widerruf der Betriebssicherheitserklärung (vgl. Art. 20).

6. Abschnitt: Bearbeitung von Personendaten

Art. 22 Informationssystem zum Betriebssicherheitsverfahren

Personen- und Firmendaten des Betriebssicherheitsverfahrens sind auf Verordnungsstufe festzulegen. Die entsprechende Liste findet sich im Anhang der VBSV.

[38] SR **172.021**
[39] SR **173.32**

Art. 23 Periodische Kontrolle der Bearbeitung von Personendaten

Das Informationssystem nach Artikel 70 Absatz 1 ISG, welches beim Betriebssicherheitsverfahren zur Anwendung kommt, kann unter Umständen besonders schützenswerte Personendaten beinhalten. Eine entsprechende unabhängige Aufsicht ist daher angezeigt. Das zuständige Departement hat bezüglich Auswahl der Revisionsstelle ein gewisses Ermessen.

7. Abschnitt: Schlussbestimmungen

Art. 24 Aufhebung und Änderung bisherigen Rechts

Absatz 1: Das nur im VBS anwendbare Geheimschutzverfahren ist in der Geheimschutzverordnung geregelt. Das bundesweit anwendbare Betriebssicherheitsverfahren deckt materiell die Regelungsmaterie der Geheimschutzverordnung ab, weshalb diese ersatzlos aufgehoben werden kann.

Absatz 2: In der VIMK wird auf die aufzuhebende Geheimschutzverordnung verwiesen, was zu korrigieren ist.

Absatz 3: Der NDB wird in Artikel 56 ISG ausdrücklich als Informationsquelle der Fachstelle BS genannt. Gemäss Artikel 60 NDG gibt der NDB Personendaten inländischen Behörden dann bekannt, wenn dies zur Wahrung der inneren oder äusseren Sicherheit notwendig ist. Der Bundesrat bestimmt die betreffenden Behörden. Dies tut er in Anhang 3 der Nachrichtendienstverordnung vom 16. August 2017[40], wo aktuell die Fachstelle BS noch nicht aufgeführt ist. Dies wird mit der vorliegenden Ziffer 10.6 nachgeholt.

Absatz 4: In den Artikeln 3 und 6 der Verordnung vom 21. November 2018[41] über die Militärische Sicherheit (VMS) sind den Organen der Militärischen Sicherheit einzelne Aufgaben mit Bezug zur Industrie zugewiesen, welche nach neuem Recht ausschliesslich durch die Fachstelle BS wahrgenommen werden. Die entsprechenden Bestimmungen sind daher zu streichen (vgl. Art. 3 VMS) oder umzuformulieren (vgl. Art. 6 VMS).

Absatz 5: Artikel 68 und Anhang 31 MIV können aufgehoben werden. Sie werden inhaltlich in der VBSV in Artikel 22 und in den Anhang aufgenommen.

Art. 25 Übergangsbestimmung

Eine Rückwirkung auf Aufträge, bei welchen die Beschaffung vor Inkrafttreten der VBSV begonnen hat, würde unter Umständen die Voraussetzungen ändern, unter welchen der Auftrag ausgeschrieben beziehungsweise zugeschlagen wurde, was in letzter Konsequenz sogar dessen Widerruf und eine Neuvergabe nach sich ziehen kann. Diese Rechtsunsicherheit ist nicht zu rechtfertigen, weshalb man es in diesen Fällen bei der vergaberechtlichen Eignung bewenden lassen soll. Für die wenigen Fälle von hängigen Geheimschutzverfahren des VBS, die zum Zeitpunkt des Inkrafttretens hängig sind, gelten sowieso in materieller Hinsicht bereits einschlägige Sicherheitsvorgaben, weshalb hier aus verfahrensökonomischen Gründen auf die in der VBSV festgehaltenen neuen Verfahrensschritte verzichtet werden soll. Betriebssicherheitserklärungen, die nach bisherigem Recht erlassen wurden, bleiben ab deren Ausstellung fünf Jahre gültig (vgl. Art. 90 Abs. 3 ISG).

Art. 26 Inkrafttreten

Das Inkrafttreten wird abgestimmt auf dasjenige der ISV und der VPSP erfolgen.

Anhang

Im Anhang finden sich nun die Daten des Informationssystems zum Betriebssicherheitsverfahren, welche gemäss Artikel 26 Absatz 5 VBSV aus der MIV entfernt werden.

5 Personelle und finanzielle Auswirkungen

5.1 Auswirkungen auf den Bund

a. ISMS und Management der Informationssicherheit (vgl. Art. 5–15 ISV)

Der Aufbau und die Einführung des ISMS *light* durch die Ämter (und die BK) wird einen moderaten, einmaligen Initialaufwand von etwa 0.5 Vollzeitstellen im Schnitt nach sich ziehen. Dieser «Projekt-

[40] SR **121.1**
[41] SR **513.61**

aufwand» wird im Amt auf mehrere Stellen (Amtsleitung, Informatik, Recht, Personal und Anwendungsverantwortliche) verteilt. Der grössere Anteil wird dennoch auf die Informationssicherheitsbeauftragten (vgl. Art. 37 ISV) zukommen. Für einen minimalen sachgerechten Betrieb des ISMS *light* in den Ämtern ist im Vergleich zu heute mit einem Zusatzaufwand von etwa 0.2 Vollzeitstellen bei den Informationssicherheitsbeauftragten zu rechnen. Die ISMS-Anwendung (vgl. Ziff. 3.8) wird die Effizienz des Betriebs des ISMS erhöhen.

Nicht alle Ämter werden den gleichen Zusatzaufwand haben. Einerseits können die Departemente und die Ämter mit entsprechenden Kostenauswirkungen ein höheres Ambitionsniveau festlegen. Andererseits erfüllen gewisse Ämter und Departemente die Vorgaben bereits. So sind einige Ämter wie armasuisse, swisstopo, BASPO, BIT und ASTRA nach ISO zertifiziert. Im VBS ist ein vollumfängliches ISMS schon seit einigen Jahren umgesetzt. Das EDI hat bereits entschieden, von seinen Ämtern die Umsetzung eines ISMS zu verlangen.

b. Sicherheitsakkreditierung von Informatikmitteln (vgl. Art. 23 ISV)

Der Aufwand für die Akkreditierung von Informatikmitteln kann zurzeit noch nicht beziffert werden. Es handelt sich um eine neue Aufgabe, mit welcher die Bundesverwaltung bisher keine Erfahrung hat. Nach der Eröffnung der Vernehmlassung wird der Bundesrat prüfen, welche Kompetenzen und Ressourcen für diese Aufgabe erforderlich sind.

c. Informationssicherheitsbeauftragte der Departemente (vgl. Art. 40 ISV)

Auf die Informationssicherheitsbeauftragten der Departemente kommt mit dem neuen Recht ebenfalls ein leicht erhöhter Aufwand von etwa 0.2 Vollzeitstellen zu. Dieser Zusatzaufwand ist teilweise auf die Steuerungs- und Koordinationsaufgaben des ISG selbst zurückzuführen. Eine weitere Ursache liegt darin, dass sie inskünftig die Einleitung von PSP bei Dritten, die nicht vom Betriebssicherheitsverfahren erfasst werden, bewilligen werden. Departemente, die viele sicherheitsempfindliche Aufträge vergeben, werden einen etwas höheren Aufwand haben.

d. Fachstelle des Bundes für Informationssicherheit (vgl. Art. 41 ISV)

Die Ressourcen der Fachstelle des Bundes für Informationssicherheit werden erst nach der Vernehmlassung ausgewiesen (vgl. Ziff. 3.8). Sollten zusätzliche Ressourcen erforderlich sein, was zurzeit noch nicht absehbar ist, so wird der Zusatzaufwand gering ausfallen.

e. Umsetzung der technischen Sicherheitsmassnahmen und deren Kontrolle

Die Kosten für die Umsetzung von technischen Sicherheitsmassnahmen und deren Kontrolle, insbesondere im Bereich der Cybersicherheit, stellen wie bereits heute normale Projekt- und Betriebskosten dar. Sie müssen entsprechend geplant und im Rahmen des ordentlichen Budgets getragen werden müssen (vgl. Art. 42 ISV). Dies schliesst die Kosten der Durchführung von Kontrollen und Audits nach Artikel 13 ISV und die Wirksamkeitsprüfungen nach Artikel 29 Absatz 3 ISV (vgl. Art. 18 Abs. 3 ISG) ein.

f. Änderung der IAMV

Der Geltungsbereich der IAMV wird auf die Verwaltungseinheiten der dezentralen Bundesverwaltung erweitert. Wenn diese ein IAM-System einsetzen wollen, werden sie die Anforderungen der IAMV erfüllen müssen. Die entsprechenden Kosten müssen in diesem Zusammenhang geplant und im Rahmen des ordentlichen Budgets getragen werden.

g. Verordnung über die Personensicherheitsprüfungen

Detaillierte Angaben zum Aufwand für die PSP werden erst nach der Vernehmlassung vorliegen, da die dafür massgebenden Funktionenlisten ab Eröffnung der Vernehmlassung erstellt werden.

h. Verordnung über das Betriebssicherheitsverfahren

Für die Durchführung des Betriebssicherheitsverfahrens hat das VBS die Ressourcen der Fachstelle für Betriebssicherheit bereits um 1.5 Vollzeitstellen erhöht. Es sind keine zusätzlichen Ressourcen erforderlich.

5.2 Auswirkungen auf die Kantone

Bei den Kosten für die Umsetzung in den Kantonen bestehen noch Ungewissheiten. Die Anwendung des ISG und der Verordnungen auf die Kantone ist allerdings beschränkt. Die Umsetzungskosten werden vorwiegend im Rahmen von Projekten oder beim Bezug von Dienstleistungen des Bundes anfallen. Sie müssen in diesem Kontext beurteilt werden. Die Arbeitssitzungen mit den

Kantonen haben gezeigt, dass die Praxis heterogen ist. Es ist ein wichtiges Ziel der Vernehmlassung, den Aufwand für die Kantone abzuschätzen.

5.3 Auswirkungen auf die Wirtschaft

Die Auswirkungen auf die Wirtschaft wurden in der ISG-Botschaft ausgewiesen. Sie fallen äusserst gering aus. Die Wirtschaft ist vom ISG und seinen Ausführungsbestimmungen betroffen, wenn Betriebe für den Bund arbeiten. Die Bundesbehörden sind verpflichtet, die Gewährleistung der Informationssicherheit im Rahmen der Zusammenarbeit mit Dritten zu stipulieren und für eine angemessene Kontrolle der Einhaltung der Vorgaben zu sorgen. Betriebe, die sicherheitsempfindliche Aufträge des Bundes erfüllen, werden zudem im Rahmen des Betriebssicherheitsverfahrens (vgl. Ziff. 4.4, Erläuterungen zur VBSV) auf deren Vertrauenswürdigkeit hin überprüft und anschliessend regelmässig kontrolliert. Die Kosten des Verfahrens betragen in der Regel weniger als 0.5% des Auftragsvolumens und werden direkt oder indirekt auf die Auftraggeberin überwälzt. Betroffen von dieser Kontrolle werden insgesamt etwa 700 Betriebe. Die Auswirkungen auf die Wirtschaft bleiben somit insgesamt sehr gering.

5.4 Andere Auswirkungen

Die Verordnungen haben keine Auswirkungen auf die Gesellschaft, die Umwelt oder andere wichtige Bereiche. Sie zeigen im positiven Sinne jedoch deutlich auf, welche Sicherheitsmassnahmen im digitalisierten Zeitalter notwendig sind, um die Sicherheit des Bundes und damit der Schweiz gerecht zu werden.