Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Generalsekretariat VBS GS-VBS
Digitalisierung und Cybersicherheit VBS

8. November 2023

Ausführungsrecht zum Informationssicherheitsgesetz

Erläuterungen

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

Inhaltsverzeichnis

Erläuterungen

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 Ausführungserlasse zum ISG wurden in Zusammenarbeit mit Vertreterinnen und Vertretern der anderen verpflichteten 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 verpflichteten Bundesbehörden und die Kantone für alle wichtigen Regelungen zur Stellungnahme einladen werde (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 wurde ein Vernehmlassungsverfahren durchgeführt, dessen Ergebnisse in die vorliegenden Vorlagen integriert wurden.

2 Grundzüge der Vorlagen

2.1 Umfang des Ausführungsrechts zum ISG

Das Ausführungsrecht zum ISG umfasst vier Verordnungen:

- eine neue Informationssicherheitsverordnung (ISV, vgl. Ziff. 3.1);
- eine Änderung der bestehenden Verordnung vom 19. Oktober 2016[3] über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV, vgl. Ziff. 3.2);
- eine neue Verordnung über die Personensicherheitsprüfungen (VPSP, vgl. Ziff. 3.3);
- eine neue Verordnung über das Betriebssicherheitsverfahren (VBSV, vgl. Ziff. 3.4).

Das Parlament hat am 29. September 2023 eine Änderung des ISG verabschiedet, mit welcher eine Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen eingeführt wird. Dadurch wird das 5. Kapitel des ISG vollständig überarbeitet. Die dazugehörige Verordnung wird derzeit durch das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) erarbeitet.

2.2 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 und die Kantone im April 2023 in der Nationalen Cyberstrategie festgelegt haben. 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 Gruppen und Ämter sind gemäss Artikel 45 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[4] (RVOG) für die Erfüllung der ihnen

[1] BBl **2020** 9975
[2] BBl **2017** 2953
[3] SR **172.010.59**
[4] SR **172.010**

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 potenzielle Auswirkungen auf die Aufgabenerfüllung bewusst berücksichtigt und priorisiert werden. 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 technische Weisungen und Standards definiert werden.

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.

2.3 Informationssicherheitsverordnung (ISV)

a. Gegenstand

Die neue Informationssicherheitsverordnung (ISV) ersetzt die bisherige Cyberrisikenverordnung vom 27. Mai 2020[5] (CyRV) und die 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 7*a* der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[7] (RVOV) werden dem ISG und der ISV nur unterstellt,

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

wenn sie klassifizierte Informationen des Bundes bearbeiten, wenn sie auf Informatikmittel der zentralen Bundesverwaltung zugreifen oder wenn sie ihre eigenen Informatikmittel durch die Leistungserbringer des Bundes betreiben lassen. In diesen Fällen müssen sie nicht das gesamte ISG und die gesamte ISV umsetzen, sondern nur diejenigen Bestimmungen, welche die Bearbeitung klassifizierter Informationen oder die Sicherheit der Informatikmittel gewährleisten. Dasselbe gilt für Organisationen nach Artikel 2 Absatz 4 RVOG, die mit Verwaltungsaufgaben betraut werden aber nicht der Bundesverwaltung angehören. Die BK und die Departemente können dennoch dezentrale Verwaltungseinheiten, die ständig sicherheitsempfindliche Tätigkeiten ausüben, dem gesamten ISG unterstellen.

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 oder auf Informatikmittel des Bundes zugreifen, gelten die entsprechenden Vorschriften des ISG und der ISV. Zu den Vorschriften des ISG und der ISV gehören auch die entsprechenden Mindestanforderungen der Fachstelle des Bundes für Informationssicherheit, namentlich die Vorschriften und technischen Mindestanforderungen für den IT-Grundschutz in der Bundesverwaltung sowie für den Schutz von klassifizierten Informationen. Die Kantone werden wie bisher 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. Die Kantone sind nicht verpflichtet, ein Informationssicherheits-Managementsystem (ISMS) umzusetzen.

d. Management der Informationssicherheit

Sämtliche Ämter, Generalsekretariate, Gruppen und die BK werden verpflichtet, ihre Informationssicherheit mittels eines ISMS umzusetzen. Ein ISMS ist kein Informatiksystem, sondern ein Führungsinstrument, das der systematischen Planung, Umsetzung, Überprüfung und Verbesserung der Informationssicherheit dient. Es umfasst die dafür nötigen Vorschriften, Verfahren, Massnahmen und Kontrollen und macht sichtbar, wem in der Organisation, welche Aufgaben, Kompetenzen und Verantwortlichkeiten zugeordnet sind. 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 Ämter und Departemente haben sich bereits entschieden, ihre Informationssicherheit systematisch nach der ISO-Norm umzusetzen. Einige davon sind formell zertifiziert. Von den Ämtern, Generalsekretariaten, Gruppen und der BK 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, weshalb der Bund inskünftig weniger klassifizieren wird. Die Kriterien sind von Natur aus offen formuliert und müssen ausgelegt werden. Für die Umsetzung werden Hilfsmittel erstellt.

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 erarbeitet und an die Standards der Europäischen Union und der NATO angeglichen.

f. Sicherheitszertifizierung von Informatikmitteln

Neu führt die ISV die Möglichkeit ein, Informationssysteme sicherheitsmässig zertifizieren zu lassen. Eine Sicherheitszertifizierung 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. Die ISV schliesst damit eine Lücke, welche die bisherige internationale Zusammenarbeit im Sicherheitsbereich erschwerte. Im Gegensatz zu den meisten Ländern, die für die elektronische Bearbeitung klassifizierter Informationen eine Zertifizierung verlangen, wird in der ISV die Zertifizierung nur dann verlangt, wenn sie für die nationale oder internationale Zusammenarbeit nötig ist.

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 Arbeitgeber, 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. Verschuldung im Spielcasino, problematische Beziehungskonstellationen oder Reisen in besondere Länder). Für die Mitarbeitenden können solche Sachverhalte psychisch sehr belastend sein. Es ist Teil der Fürsorgepflicht des Arbeitsgebers nach Artikel 4 Absatz 2 Buchstabe g BPG, dass er seinen Angestellten zuhört und mit ihnen versucht die Risikoexposition zu mindern. Der Umgang mit einem allenfalls erhöhten Risiko bleibt letztendlich 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. Informationssicherheitsverantwortliche 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 (Informationssicherheitsverantwortliche). Die Informationssicherheitsverantwortlichen beaufsichtigen das ISMS des Amts und treffen alle wichtigen Entscheide im Bereich Informationssicherheit. Die operativen Aufsichtstätigkeiten sind Aufgabe der Informationssicherheitsbeauftragten gemäss Artikel 37 ISV. Mit der ISV werden die bisherigen 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.

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

Das ISG schafft eine Fachstelle des Bundes für Informationssicherheit. Artikel 83 ISG legt ihre Aufgaben für die Zusammenarbeit mit den vom Bundesrat unabhängigen verpflichteten Behörden fest. Diese Aufgaben sind vorwiegend unterstützend und koordinierend. Die ISV legt ihre Aufgaben für den Zuständigkeitsbereich des Bundesrates fest. Die Fachstelle wird für die Bundesverwaltung und die Armee die nötigen organisatorischen, personellen, technischen und baulichen Vorgaben zur Gewährleistung der Informationssicherheit nach dem Stand der Technik beschliessen. Sie wird zudem die BK und die Departemente beim Sicherheitsmanagement unterstützen. Im internationalen Verhältnis wird die Fachstelle die Rolle der nationalen Sicherheitsbehörde der Schweiz wahrnehmen (vgl. dazu ISG-Botschaft, Ziff. 5.2 sowie Art. 42 Abs. 3 ISV). Die Fachstelle des Bundes für Informationssicherheit ist Teil des Staatssekretariats für Sicherheitspolitik (SEPOS) im VBS. Sie übernimmt die Aufgaben des Bundesamts für Cybersicherheit (BACS) in Bezug auf den Eigenschutz des Bundes (Vorgaben und Beratung).

[8] SR **172.220.1**

Das BACS fokussiert sich auf den Schutz der Schweiz vor Cyberrisiken. Mit der Einführung einer Meldepflicht bei Cybervorfällen im ISG wird das BACS seine Leistungen zugunsten der kritischen Infrastrukturen, der Wirtschaft und der Bevölkerung ausbauen. Es wird aber weiterhin die BK, Departemente und Ämter bei Fragen zur Cybersicherheit, einschliesslich beim Erlass von technischen Vorgaben, beraten und unterstützen. Die Bundesbehörden sind mit der Änderung des ISG ebenfalls verpflichtet, dem BACS Cybervorfälle zu melden. Sofern die Departemente und die Ämter nicht in der Lage sind, einen Vorfall selber zu bewältigen, wird das BACS sie dabei unterstützen oder nach Rücksprache mit der Fachstelle des Bundes für Informationssicherheit sogar die Federführung übernehmen.

Da beim Inkrafttreten des ISG die Fachstelle des Bundes für Informationssicherheit noch nicht operationell sein wird, wird das BACS bis Mitte 2025 seine bisherigen Aufgaben im Bereich Eigenschutz des Bundes (Informatiksicherheit Bund) wahrnehmen.

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

Bis anhin stützte sich die IAMV in erster Linie auf das RVOG. Mit den Artikeln 24–26 ISG wird nun eine spezifische formell-gesetzliche Grundlage geschaffen, auf der die IAMV fortan basieren wird. Gestützt auf Artikel 20 Absatz 2 ISG wird es zudem unter bestimmten Voraussetzungen zulässig sein, in IAM-Systemen biometrische Daten neu generell zu verwenden. In der Folge sind in der IAMV die notwendigen Anpassungen vorzunehmen.

Als Teil des Standarddienstes eIAM hat die Bundesverwaltung einen Authentisierungsdienst für den Zugriff auf ihre Fachanwendungen und E-Government Dienstleistungen aufgebaut. Dieser Dienst hat sich bewährt und soll gestützt auf das Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG) auch den interessierten Kantonen (und ihren Gemeinden) zur Integration mit ihren Anwendungen zur Verfügung gestellt werden. In der Folge sind in der IAMV die notwendigen Anpassungen vorzunehmen.

Im Rahmen dieser Vorlage erfährt die IAMV nur diejenigen Änderungen, die aufgrund des ISG und des EMBAG notwendig sind. Der identifizierte weitere Anpassungsbedarf der IAMV hingegen ist nicht Teil dieser Vorlage, sondern Gegenstand einer Totalrevision, die die BK bereits an die Hand genommen hat.

2.5 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, die Wirksamkeit der PSP zu verstärken, indem die Palette der Daten, auf welche die Fachstellen PSP zur Beurteilung des Sicherheitsrisikos zugreifen dürfen, erweitert wird. Der Bundesrat will im Gegenzug, dass die PSP nach neuem Recht für Funktionen vorbehalten wird, die tatsächlich ein erhebliches Risiko für den Bund oder die Armee darstellen können. Damit sollen künftig deutlich weniger PSP durchgeführt werden. Die PSP müssen fachgerecht mit den bestehenden Ressourcen innert nützlicher Frist bewältigt werden können. Das neue Recht setzt also auf Qualität anstatt auf Quantität. 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].

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

Materiell regelt die Verordnung sowohl die PSP nach dem ISG als auch alle anderen Prüfungen, Beurteilungen und Kontrollen, die zwar nicht im 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.

c. Geltungsbereich

Die VPSP gilt grundsätzlich für alle Behörden und Organisationen, die dem ISG unterstehen. Für die dezentralen Verwaltungseinheiten und Organisationen mit Verwaltungsaufgaben nach Artikel 2 Absatz 4 RVOG ist der Geltungsbereich eingeschränkt: Nur diejenigen, die unter den Geltungsbereich der ISV fallen, fallen bezüglich PSP nach ISG auch unter den Geltungsbereich der VPSP. Dezentrale Verwaltungseinheiten, die vom Geltungsbereich des BPG erfasst werden, können ebenfalls von den Prüfungen der Vertrauenswürdigkeitsprüfungen nach Artikel 20*b* BPG betroffen sein und in diesem Zusammenhang unter den Geltungsbereich der VPSP fallen.

Die VPSP gilt auch für die vom Bundesrat unabhängigen verpflichteten Bundesbehörden nach Artikel 2 Absatz 1 ISG. Der Gesetzgeber hat nämlich in Artikel 48 ISG dem Bundesrat die alleinige Kompetenz erteilt, die Modalitäten des Prüfverfahrens und der Organisation der Fachstellen PSP zu regeln. Hingegen bleiben die verpflichteten Behörden für den Erlass ihrer Funktionenlisten oder für die Bezeichnung der einleitenden und entscheidenden Stellen zuständig.

d. 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.

e. 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 bisher. Das VBS wird deshalb die Funktionenlisten zentral bewirtschaften und sie auf Antrag der Departemente und der BK laufend aktualisieren.

Die Listen der Funktionen, für die eine PSP nach dem ISG erforderlich sind, 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, werden daher gestützt auf Artikel 6 des Publikationsgesetzes vom 18. Juni 2004[13] (PublG) nicht veröffentlicht. Aus denselben Gründen werden die Funktionenlisten nach dem Stromversorgungsgesetz vom 23. März 2007[14] (StromVG) ebenfalls nicht veröffentlicht. Hingegen werden die Listen der Funktionen, die in erster Linie zum Schutz vor Korruption oder vor Reputationsschaden einer Prüfung unterstellt werden, wie bis anhin veröffentlicht.

2.6 Verordnung über das Betriebssicherheitsverfahren (VBSV)

a. Allgemeines

Das ISG (vgl. Art. 49–72) führt das sogenannte Betriebssicherheitsverfahren ein. Das Verfahren befasst sich mit der Wahrung der Informationssicherheit bei der Vergabe von sicherheitsempfindlichen Aufträgen der Bundesbehörden an Unternehmen (Betriebe), die nicht ihrer unmittelbaren Aufsicht unterstehen. Das Verfahren dient der Prüfung der Vertrauenswürdigkeit des zu beauftragenden Unternehmens. Firmen, die unter Einfluss von ausländischen Nachrichtendiensten stehen,

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

sollen keinen Zugang zu sicherheitsempfindlichen Informationen oder zu kritischen Informatikmitteln des Bundes erhalten. 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. 2.3 Bst. b).

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 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.

2.7 Übergangsfristen

Für einen erfolgreichen Übergang in das neue Recht sehen sowohl das ISG als auch seine Ausführungsverordnungen angemessene Übergangsfristen vor. Folgende Übergangsfristen gelten für die Ämter, Generalsekretariate, Gruppen und die BK ab Inkrafttreten des ISG:

- 1 Jahr, um in einem Klassifizierungskatalog festzuhalten, wie Informationen in ihrem Zuständigkeitsbereich gemäss neuen Recht zu klassifizieren sind (vgl. Art. 51 Abs. 5 ISV);
- 2 Jahre, um eine Schutzbedarfsanalyse durchzuführen und ihre Informatikmittel gemäss neuem Recht einzustufen (vgl. Art. 90 Abs. 2 ISG);
- 3 Jahre, um:
  - ihr ISMS aufzubauen (vgl. Art. 51 Abs. 4 ISV),
  - ihre Funktionenliste zu den PSP zu überprüfen (vgl. Art. 6 Abs. 1 VPSP);
- 6 Jahre (ein LifeCycle), um die neuen technischen Sicherheitsvorschriften für sämtliche Informatikmitteln umzusetzen (vgl. Art. 90 Abs. 2 ISG).

[15] SR **510.413**

3 Erläuterungen zu einzelnen Artikeln

3.1 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 den 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. Unter den Begriff «Information» werden auch Daten subsumiert. Wenn Personendaten im Sinne der Datenschutzgesetzgebung gemeint sind, wird jeweils der Begriff «Personendaten» verwendet.

Das Verhältnis zwischen dem ISG und dem ausser Kraft gesetzten DSG vom 19. Juni 1992 (aDSG) ist in der Botschaft zum ISG ausführlich erläutert (vgl. ISG-Botschaft, Ziff. 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 1–3: Die ISV gilt für den Bundesrat, die zentrale Bundesverwaltung und die Armee.

Grundsätzlich fallen alle Verwaltungseinheiten der dezentralen Bundesverwaltung nach Artikel 7*a* der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[16] (RVOV) sowie Organisationen nach Artikel 2 Absatz 4 RVOG, die mit Verwaltungsaufgaben betraut werden, aber nicht der Bundesverwaltung angehören, unter den Geltungsbereich des ISG (vgl. Art. 2 Abs. 2 ISG). Artikel 2 Absätze 3 und 4 ISG erteilen dem Bundesrat allerdings die Kompetenz, die Geltung des Gesetzes auf gewisse Organisationen oder auf Teile des Gesetzes einzuschränken. Das Gesetz räumt ihm dabei einen Ermessensspielraum ein, um die Vollzugsautonomie der betreffenden Organisationseinheiten zu berücksichtigen. Mit der Regelung von Artikel 2 Absätze 2 und 3 ISV nutzt der Bundesrat seinen Ermessensspielraum aus, indem die betreffenden Organisationen für das Einsetzen eigener Informatikmittel, unabhängig von deren Schutzstufe, vom Geltungsbereich des ISG ausgenommen werden, während sie in zwei anderen Teilbereichen dem ISG unterstellt bleiben. Durch die Einschränkung der Bestimmungen gestützt auf Artikel 2 Absatz 4 ISG im Zuständigkeitsbereich des Bundesrates wird zur Wahrung der Vollzugsautonomie und aus Kostengründen der Fokus auf die Informationssicherheit der zentralen Bundesverwaltung und der Armee gelegt.

Die Verwaltungseinheiten der dezentralen Bundesverwaltung werden demzufolge dem ISG und der ISV nur dann unterstellt, wenn sie klassifizierte Informationen des Bundes bearbeiten, wenn sie auf Informatikmittel der zentralen Bundesverwaltung zugreifen oder wenn sie ihre eigenen Informatikmittel durch die Leistungserbringer des Bundes betreiben lassen. In diesen Fällen müssen sie nicht das gesamte ISG und die gesamte ISV umsetzen, sondern nur diejenigen Bestimmungen, welche die Bearbeitung klassifizierter Informationen oder die Sicherheit der Informatikmittel gewährleisten. Dasselbe gilt für Organisationen nach Artikel 2 Absatz 4 RVOG, die mit Verwaltungsaufgaben betraut werden, aber nicht der Bundesverwaltung angehören. Mit dieser pragmatischen Lösung werden die dezentralen Verwaltungseinheiten nur dann verpflichtet, wenn ihre Tätigkeiten eine Gefährdung der zentralen Bundesverwaltung darstellen können.

Die BK und die Departemente können allerdings entscheiden, dass die ihnen unterstellten dezentralen Verwaltungseinheiten dem gesamten ISG unterstellt werden müssen. Voraussetzung dafür ist, dass diese Verwaltungseinheiten oder Organisationen ständig sicherheitsempfindliche Tätigkei-

[16] SR **172.010.1**

ten nach Artikel 5 Buchstabe b ISG ausüben. Im VBS trifft dies zum Beispiel auf die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten zu, welche täglich «geheim» klassifizierte Informationen der Nachrichtendienste bearbeitet. Die Unterstellung führt zu den gleichen Aufgaben und Verantwortlichkeiten, wie sie die Bundesämter der zentralen Bundesverwaltung durch das ISG und die ISV erhalten. Sie müssen insbesondere auch ein ISMS betreiben.

Für die anderen verpflichteten Behörden nach Artikel 2 Absatz 1 Buchstabe a sowie c–e ISG (die Bundesversammlung, die eidgenössischen Gerichte, die Schweizerische Bundesanwaltschaft und ihre Aufsichtsbehörde sowie die Schweizerische 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 (vgl. hingegen die Geltung der VPSP und der VBSV).

Absatz 4: 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. 34). 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 in der Bundesverwaltung (Si001) 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 kantonalen Verwaltungen auch öffentlich-rechtliche Körperschaften, Anstalten oder Stiftungen erfasst, die dem Verwaltungsrecht des entsprechenden Kantons unterstehen. Es ist seitens der 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 eine kantonale Organisation nicht unter den Geltungsbereich des ISG, wird sie als Dritte im Sinne von Artikel 9 ISG behandelt (vgl. Erläuterungen zu Art. 10).

Absatz 4 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.

Absatz 5: Die ISV gilt auch für die Armee. Die Aufgaben, Kompetenzen und Verantwortungen werden aber wie bis anhin durch die Militärverwaltung übernommen, was durch die neue Gesetzgebung weiterhin bestehen bleiben soll.

2. Abschnitt: Grundsätze

Art. 3 Sicherheitsziele

Die Informatikmittel der zentralen Bundesverwaltung und der Armee 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.

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 Auswirkun-

gen) 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 sind die Direktorinnen und Direktoren der Gruppen und Ämter 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 legte bisher das BACS minimale Informationssicherheitsvorgaben fest, insbesondere den IT-Grundschutz in der Bundesverwaltung, welche dem Schutz der gesamten Bundesverwaltung dienen und die Ämter, Generalsekretariate, Gruppen und die BK mit beschränktem Handlungsspielraum umsetzen müssen. Diese entbinden sie jedoch nicht von ihrer Verantwortung, die Risiken laufend zu beurteilen und, wenn nötig, weitergehende Massnahmen zu treffen. Um diesen Schutz der gesamten Bundesverwaltung gewähren zu können, sollen auch die Kantone, welche klassifizierte Informationen des Bundes bearbeiten oder auf dessen Informatikmittel zugreifen, sich an diese Anforderungen halten müssen (vgl. Erläuterungen zu Art. 49).

Absatz 3: Bei der Bearbeitung von Informationen oder bei der Nutzung von Informatikmitteln des Bundes, müssen die Mitarbeitenden die entsprechenden Verhaltensvorschriften einhalten. Die Wahrnehmung dieser Verantwortung setzt voraus, dass sie entsprechend instruiert und ausgebildet werden sowie über die notwendigen Mittel verfügen (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 und zu überprüfen.

Absatz 4: Die Vorgesetzten aller Stufen tragen auch im Bereich der Informationssicherheit die Verantwortung für die funktionsbezogene, praxisnahe Instruktion und Ausbildung ihrer Mitarbeitenden bzw. unterstellten Angehörigen der Armee 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 Ämter, Generalsekretariate, Gruppen und der BK, 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 BK, der Departemente und der Fachstelle des Bundes für Informationssicherheit fest. Die Fachstelle wird dazu Vorgaben erlassen und die nötigen Hilfsmittel bereitstellen. Das BACS erbringt wichtige Leistungen zugunsten des Sicherheitsmanagements der Bundesverwaltung, insbesondere bei der Bewältigung von Cybervorfällen (vgl. Art. 12).

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 (vgl. Ziff. 2.3 Bst. d).

Während die Informationssicherheitsverantwortlichen der Verwaltungseinheiten (vgl. Art. 36) den Aufbau, den Betrieb, die Überprüfung und die kontinuierliche Verbesserung des ISMS sicherstellen, obliegt der eigentliche Betrieb des ISMS den Informationssicherheitsbeauftragten der Verwaltungseinheiten (vgl. Art. 37 Abs. 2 Bst. a). Die Letzteren werden von den Verantwortlichen beauftragt.

Gemäss Artikel 51 Absatz 4 muss ein ISMS bis spätestens drei Jahre nach Inkrafttreten der ISV aufgebaut sein.

Absatz 2: Ein ISMS bezweckt, die Informationssicherheit in der Organisation 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.

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 bzw. von der BK unabhängigen Stelle oder vom Departement verlangt. Diese unabhängige ISMS-Überprüfung sorgt für die kontinuierliche Verbesserung der Sicherheit und schafft gleichzeitig Vertrauen für die Partner des Amts. Das Amt bzw. die BK entscheidet, wie sie mit den Befunden der Überprüfung umgehen will und welche Massnahmen sie umsetzen will. Der kontinuierliche Verbesserungsprozess ist für die Gewährleistung der Informationssicherheit zentral. Diesem wird mit solchen Überprüfungen Rechnung getragen.

Die Periodizität von drei Jahren richtet sich zwar nach dem offiziellen Zertifizierungszyklus der ISO-Norm (ISO/IEC 27001), 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).

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

Ein Verzeichnis über die im eigenen Zuständigkeitsbereich massgebenden Rechtsgrundlagen sowie vertraglichen Verpflichtungen im Bereich Informationssicherheit dient dem Nachweis der Einhaltung der relevanten Rechtsgrundlagen, welche beispielsweise im Rahmen der Messung der jährlichen Zielerreichung des ISMS (vgl. Art. 5 Abs. 2 oder der ISMS-Überprüfung nach Art. 5 Abs. 3) geprüft wird. 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.

Die Fachstelle berät die Verwaltungseinheiten in Sicherheitsfragen unter anderem auch bei der Pflege der sicherheitsrelevanten 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: Die CyRV kannte 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. Mehrere gleiche oder zusammenhängende Schutzobjekte können auch zu einem einzelnen zusammengefasst werden. 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 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 e: Die Umsetzung der Sicherheitsmassnahmen muss nicht zwingend im Inventar selbst dokumentiert werden. Im Inventar muss aber zumindest festgehalten werden, wo die Sicherheitsdokumentation zu finden ist und wer dafür zuständig ist.

Absatz 3 Buchstabe f: Vgl. Erläuterungen zu Artikel 13 in Verbindung mit Artikel 5 Absätze 2 und 3.

Absatz 3 Buchstabe g: Die Möglichkeit der geteilten Nutzung der jeweiligen Schutzobjekte verweist auf das «Once-Only-Prinzip». Dabei entscheiden die Verwaltungseinheiten in eigenem Ermessen, welche Schutzobjekte mit anderen Verwaltungseinheiten geteilt werden. Wenn das Schutzobjekt Personendaten enthält, müssen selbstverständlich alle beteiligten Verwaltungseinheiten über die nötigen Rechtsgrundlagen verfügen, um auf diese Daten zuzugreifen und sie zu bearbeiten.

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.

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 zur Pflege der Rechtsgrundlagen und vertraglichen Verpflichtungen nach Artikel 6.

Absatz 1 Buchstabe d: Verlangt wird ein bewusster Entscheid des Informationssicherheitsverantwortlichen, das heisst die nachweisbare Akzeptanz von Restrisiken auf Grundlage eines sorgfältig durchlaufenen Analyse- und Entscheidungsprozesses. Die Nachweisbarkeit ist an keine bestimmte Form gebunden. Damit soll im Kontext der Digitalisierung der Einsatz technologieneutraler Nachweismethoden ermöglicht werden.

Absatz 3: Massgebend sind die Weisungen über die Risikopolitik des Bundes sowie die damit verbundenen Richtlinien und Handbücher. Die Ämter berichten ihrem Departement, welches daraufhin dem Bundesrat Bericht erstattet. Die Konsolidierung erfolgt durch die Koordinationsstelle Risikomanagement Bund und die GSK.

Art. 9 Bewilligung und Verzeichnung von Ausnahmen

Wie bereits zuvor mit dem BACS, wird mit der Inkraftsetzung der ISV die Fachstelle des Bundes für Informationssicherheit gestützt auf Artikel 85 ISG vorgeben, welche Mindestanforderungen im Bereich Informationssicherheit erfüllt werden müssen. In diesen Vorgaben wird sie auch festlegen, wer über die Ausnahmen der Einhaltung von Mindestvorgaben entscheidet. Grundsätzlich wird das bisherige Verfahren der CyRV über die Ausnahmebewilligungen übernommen.

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). Die Beurteilung der Sicherheitsrisiken richtet sich nach den Vorgaben von Artikel 8 ISV.

Absatz 3: Mehrere Vorfälle bei externen Partnern des Bundes haben gezeigt, dass diese den gleichen Sicherheitsstandard wie die Bundesbehörden einhalten müssen, wenn sie Informationen des Bundes bearbeiten oder für den Bund Informatikdienstleistungen erbringen. Deshalb müssen die Verträge mit Dritten klare Anforderungen an die Informationssicherheit und deren Überprüfung stellen. Die Verträge müssen unter anderem die Pflicht beinhalten, den Schutz der Informationen und Daten des Bundes gemäss Bundesstandard (inkl. Datenschutzanforderungen, vgl. ISG-Botschaft zu Art. 9) zu gewährleisten und sicherheitsrelevante Ereignisse zu melden. In den Verträgen müssen ebenfalls die Modalitäten des Nachweises der Umsetzung der Sicherheitsvorgaben stipuliert und insbesondere ein Auditrecht für den Bund eingeräumt werden.

Art. 11 Schulung und Sensibilisierung

Wenn die Bundesverwaltung und die Armee ihre Sicherheit nachhaltig verbessern wollen, müssen sie ihre Mitarbeitenden und Angehörigen (darunter auch die Vorgesetzten) so sensibilisieren und schulen, dass sie nicht nur die präventiven Sicherheitsmassnahmen vorschriftskonform umsetzen, sondern auch in der Lage sind, Gefahren und Bedrohungen selber zu erkennen, korrekt zu reagieren und entsprechende Sicherheitsmeldungen zu erstatten.

Die Verwaltungseinheiten stellen die generelle Schulung (wie regelmässige Sensibilisierungs- und Awareness-Kampagnen oder Eintrittsschulungen) für sämtliche Mitarbeitende sowie das notwendige Budget, die Zeit und entsprechende Ressourcen sicher. Dies ergänzend zu den direkten Vorgesetzten, die 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 Behandlung der Sicherheitslücken sind die Verwaltungseinheiten verantwortlich. Sie müssen deshalb im Rahmen ihres ISMS im Amt und mit den Leistungserbringern die Meldung von Sicherheitsereignissen und die Reaktion darauf festlegen. Als «Sicherheitsvorfall» gilt ein Ereignis, bei dem die Informationssicherheit oder die entsprechenden Sicherheitsvorgaben verletzt werden oder wurden. Als «Sicherheitslücke» gilt 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 auf das Geschäft verfügen.

Absatz 2: Diese Bestimmung deckt sich mit dem bisherigen Recht (vgl. Art. 14 Abs. Abs. 4 Bst. c CyRV).

Absatz 3: Im Zusammenhang mit dem Aufbau und dem Betrieb des ISMS werden die Ämter und ihre Departemente sowie die BK befähigt, Vorfälle professionell nach einem systematischen Ansatz zu bewältigen. Sowohl die Fachstelle des Bundes als auch das BACS können die Verwaltungseinheiten und Departemente dabei beraten oder unterstützen. Das BACS wird sich wie bisher auf die Beratung im Bereich der Cybersicherheit fokussieren; die Fachstelle wird ihrerseits eine breite allgemeine Beratung im Bereich Sicherheitsmanagement anbieten sowie fachspezifische Fragen in den Bereichen Sicherheitsrecht, Industriesicherheit oder Personensicherheit beantworten können. Mit der Kann-Vorschrift wird betont, dass die Fachstelle des Bundes für Informationssicherheit und das BACS unterstützend tätig sein können, aber eben nicht müssen. Die Unterstützung der beiden Stellen erfolgt grundsätzlich auf Anfrage der Verwaltungseinheiten oder der Departemente. Die Unterstützung wird selbstverständlich nach der Kritikalität und der Wichtigkeit des Vorfalls sowie nach den zur Verfügung stehenden Ressourcen priorisiert.

Absätze 5–7: Wenn ein Vorfall eine höhere Dimension erreicht hat oder erreichen könnte, müssen die Ämter und Departemente eine Meldung an die Fachstelle erstatten. Die Kriterien nach Absatz 5 betreffen Vorfälle, bei denen nicht nur die Interessen und Aufgaben des Amts oder Departements beeinträchtigt werden können, sondern der gesamten Bundesverwaltung. Die hohe politische Bedeutung eines Vorfalls hängt sowohl von den betroffenen Informationen, Informatiksystemen oder Organisationen als auch von den Umständen des Vorfalls ab. Die politische Bedeutung eines Vorfalls hat die Tendenz, sich dynamisch zu verändern. Diese wird zusammen mit der für die Informationssicherheit verantwortlichen Person des entsprechenden Amts oder Departements geprüft.

Wenn ein Vorfall «kritisch» im Sinne der Kriterien von Absatz 5 ist, prüft die Fachstelle mit der betroffenen Verwaltungseinheit und, wenn die Cybersicherheit betroffen ist zusätzlich mit dem BACS, ob Unterstützung oder sogar eine Übernahme der Federführung nötig ist. Wenn Gefahr

in Verzug besteht, wird dieser Entscheid sehr schnell getroffen. Je nach Ausprägung des Vorfalls oder der entdeckten Schwachstelle kann entweder die Fachstelle oder das BACS die Federführung übernehmen. Mit «Federführung» ist die operative Entscheidungskompetenz gemeint. Die Verantwortung für die Informationssicherheit trägt jedoch nach wie vor die betroffene Verwaltungseinheit oder das betroffene Departement (vgl. Erläuterungen zu Art. 4). Wenn die Fachstelle oder das BACS die Federführung übernimmt, kann sie oder es beispielsweise Sofortmassnahmen anordnen oder den Einsatz von Spezialisten zur Unterstützung einsetzen. In diesem Zusammenhang anfallende Kosten gehen zu Lasten der verantwortlichen Verwaltungseinheit oder des Departements und erfolgen in Rücksprache mit diesen.

Mit der Einführung der Meldepflicht bei Cybervorfällen (vgl. Ziff. 2.1 oben) müssen die Bundesbehörden wie alle anderen kritischen Infrastrukturen dem BACS Meldung erstatten, wenn sie Opfer eines Cyberangriffs sind. Das VBS wird dafür sorgen, dass die Meldung an das BACS und an die Fachstelle koordiniert wird und dass die Prozesse bei der Bewältigung von Sicherheitsvorfällen klar, effizient und wirksam sind. Zur Datenbearbeitung im Rahmen des Vorfallmanagements vgl. Artikel 44–46 ISV.

Art. 13 Planung von Kontrollen und Audits

Eine wesentliche Lücke im Management der Informationssicherheit der Bundesverwaltung und der Armee sind 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 im nächsten 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 Informationssicherheitsverantwortliche oder den Informationssicherheitsverantwortlichen 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 weniger Aufwand durchgeführt werden können und oft günstiger sind als Audits. Zum Bespiel kann eine ein Amt oder die BK 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 betreffen auch die Einhaltung der Vorschriften bei Dritten, beispielsweise bei Lieferanten. Alle Verträge mit Dritten sollen ein Auditrecht für den Bund einräumen (vgl. auch Art. 10 Abs. 3). 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 seine Ressourcen sinnvoll einsetzt und 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

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. 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 die BK oder das Departement 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. Die Fachstelle des Bundes für Informationssicherheit legt die Modalitäten der Berichterstattung fest.

Absatz 3: Gemäss Artikel 83 Absatz 1 Buchstabe h ISG erfasst der Bericht an den Bundesrat ebenfalls den Stand der Sicherheit bei den anderen verpflichteten Behörden, weshalb die Berichterstattung mit ihnen koordiniert werden muss. Dies wird in erster Linie im Rahmen der Konferenz nach Artikel 82 ISG stattfinden.

Art. 15 Vorgaben zum Management der Informationssicherheit

Dieser Artikel bezieht sich auf Artikel 85 ISG. Die Fachstelle erhält vom Bundesrat die Aufgabe, die Vorgaben zum Management der Informationssicherheit (Art. 5–14) für die Bundesverwaltung und die Armee zu erlassen. Zur Übergangsbestimmung: vgl. Artikel 50 Absatz 6.

4. Abschnitt: Klassifizierte Informationen

Die Artikel 18–20 beschreiben die materiellen Voraussetzungen für die Klassifizierung von Informationen (vgl. ISG-Botschaft zu Art. 13). Diese sind weitgehend mit den Kriterien, die im Rahmen des Risikomanagements des Bundes für die Beurteilung des Schadenausmasses eines Ereignisses gelten, harmonisiert. Im Vergleich zur bisherigen ISchV werden dadurch die Schwellenwerte für die Klassifizierung INTERN, VERTRAULICH und GEHEIM erhöht. Mit dieser Erhöhung soll es künftig möglich sein, die Informationen zielgerichteter zu klassifizieren und sie im Gegenzug besser zu schützen.

Art. 16 Grundsätze

Absatz 1: Die Klassifizierung ist zwingend, sofern die entsprechenden Kriterien nach den Artikeln 18 ff. 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 nicht klassifizierten Informationen oder Informationsträgern (wie Papiere und elektronische Speichergeräte mit Text-, Bild- oder Tondateien) kann ein Sammelwerk entstehen, welches einen höheren Schutzbedarf aufweist als eine darin enthaltene isolierte Information. Dies ist typischerweise bei Datenbanken der Fall.

Ob ein amtliches Dokument basierend auf dem Öffentlichkeitsprinzip beispielsweise einer Journalistin oder einem Journalisten ausgehändigt wird, hängt nicht von seinem allfälligen Klassifizierungsvermerk ab, sondern bestimmt sich einzig nach den Kriterien des Öffentlichkeitsgesetzes vom 17. Dezember 2004[17] (BGÖ). Die Kriterien, welche eine Klassifizierung von Informationen begründen, sind mit den Kriterien von Artikel 7 BGÖ, welche eine Einschränkung, Aufschiebung oder Verweigerung des Zugangs zu amtlichen Dokumenten begründen, harmonisiert. Massgebend ist in jedem Fall die bundesgerichtliche Rechtsprechung zum Geheimnisbegriff, insbesondere zur Unterscheidung zwischen formellem und materiellem Geheimnis.

Im Übrigen gelten für amtliche Dokumente des Bundes, wie klassifizierte Informationen des Bundes, die kantonalen Öffentlichkeitsgesetze grundsätzlich nicht. Entsprechende Zugangsgesuche richten sich ausschliesslich nach dem Bundesrecht. Erhält beispielsweise ein Kanton ein Zugangsgesuch zu einer klassifizierten Information des Bundes, so ist diejenige Bundesstelle zu konsultieren, welche für den Schutz der klassifizierten Information zuständig ist.

Art. 17 Klassifizierende Stellen

Absatz 1: Die Ämter, Generalsekretariate, Gruppen, BK und die Departemente (bzw. die für sie handelnden Organe) sind diejenigen Stellen, die in ihrem Zuständigkeitsbereich am besten beurteilen können, für welche Informationen ein objektiv gerechtfertigtes Schutzinteresse besteht. Sie sind damit die eigentlichen klassifizierenden Stellen mit den umfassenden Kompetenzen zur Klassifizierung sowie deren Abänderung und Aufhebung (Art. 12 Abs. 2 ISG). Mit Absatz 1 werden sie beauftragt, in einem Klassifizierungskatalog diese Informationen für ihren Zuständigkeitsbereich möglichst umfassend aufzuführen. Dazu gehört auch die voraussichtliche Dauer der Klassifizierung.

[17] SR **152.3**

Da diese zu klassifizierenden Informationen ständig bearbeitet werden, kann im Voraus meistens festgelegt werden, bis wann die Information auf welcher Stufe klassifiziert sein soll. Die Verordnung gibt keine minimale oder maximale Frist vor. Die Festlegung der Klassifizierungsfrist entbindet nicht von der Pflicht nach Artikel 25, im konkreten Fall den Schutzbedarf eines bestimmten Dokuments alle 5 Jahre zu überprüfen.

Die Klassifizierungskataloge der Verwaltungseinheiten sind für die Mitarbeitenden materiell verbindlich. Sie müssen die darin enthaltenen Informationen entsprechend formell klassifizieren, in dem sie das Klassifizierungsvermerk auf das Dokument anbringen (vgl. Abs. 5). Wenn die Klassifizierung offensichtlich falsch ist, so ist die Regelung von Artikel 24 ISV anzuwenden.

Absatz 2: Mit dieser Überprüfung soll sichergestellt werden, dass bei der Erstellung der Klassifizierungskataloge die gesetzlichen Kriterien für die Klassifizierung innerhalb der Bundesverwaltung nach vergleichbaren Massstäben angewendet werden. Die abschliessende Entscheidkompetenz der Ämter, Generalsekretariate, Gruppen, BK und der Departemente bleibt erhalten.

Absatz 3: In der Bundesverwaltung und der Armee werden viele Informationen bearbeitet, die nicht spezifisch einem Amt oder einem Departement zugewiesen werden können (z.B. Objekt- und Personenschutz, Informatikmittel, Bundesratsgeschäfte). Um diesen allgemeinen verbindlichen Klassifizierungskatalog soll sich die Fachstelle des Bundes für Informationssicherheit kümmern.

Absatz 4: Die Klassifizierungskataloge nach den Absätzen 1 und 3 enthalten keine abschliessenden Aufzählungen. Wer Informationen bearbeitet, wird irgendwann in die Situation geraten, dass sie oder er zwar eine Information als schutzwürdig beurteilt, diese in den Katalogen aber nicht findet. Den Mitarbeitenden des Bundes und den Angehörigen der Armee (Bst. a) obliegt in diesem Fall die Pflicht, die fragliche Information entweder in Analogie zu einem Eintrag in einem Klassifizierungskatalog neu aufzunehmen oder direkt anhand der Klassifizierungskriterien nach den Artikeln 18–20 zu klassifizieren. Die gleiche Pflicht trifft Auftraggeberinnen, wenn sie Dritte mit der Bearbeitung schutzwürdiger Informationen betrauen (Bst. b).

Absatz 5: Allgemein gilt es sicherzustellen, dass die schutzwürdige Information genau ab dem Zeitpunkt, ab dem sie optisch und/oder akustisch wahrnehmbar ist, geschützt wird. Dies ist der Fall, sobald sie sich auf einem Informationsträger befindet. Es ist daher wichtig, dass der Schutz unmittelbar an der Quelle greift und von allen Personen, die mit der Bearbeitung befasst sind, durch die formelle Kennzeichnung (Anbringen des Klassifizierungsvermerks) vorgenommen wird. Eine Sonderform dieser Kennzeichnung gilt für den mündlichen Austausch von Informationen, indem vorgängig darauf aufmerksam gemacht wird, dass demnächst klassifizierte Informationen mündlich bekannt gegeben werden. Die Personen nach Absatz 5 haben nicht das Recht, eine Klassifizierung der Information herabzusetzen oder aufzuheben. Diese Kompetenz verbleibt stets bei den Ämtern, der BK und den Departementen.

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 vorliegen. 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 320 des Strafgesetzbuchs vom 21. Dezember 1937[18] 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.

[18] SR **311.0**

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.

Art. 21 Bearbeitungsvorgaben

Absätze 1 und 2: 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. Es handelt sich dabei um einheitliche Mindestvorgaben, die an die Vorgaben ausländischer Partner der Schweiz anzugleichen sind (vgl. Abs. 3 sowie Art. 3 Abs. 3 ISV). Für dezentrale Verwaltungseinheiten und Organisationen nach Artikel 2 Absatz 4 RVOG gelten die Anforderungen, wenn sie klassifizierte Informationen des Bundes bearbeiten oder das Departement sie dem Geltungsbereich des ISG unterstellt. Die Verwaltungseinheiten und die Armee können für ihren Zuständigkeitsbereich einen höheren Schutz festlegen. Sie können die Einhaltung allfälliger erhöhter Schutzmassnahmen aber von den anderen Organisationen des Bundes nicht verlangen, wenn sie ihre klassifizierten Informationen mit anderen austauschen wollen oder müssen, da dies den Grundsatz eines einheitlichen Standards sonst verletzen würde.

Absatz 3: In Anwendung von Artikel 84 Absatz 1 ISG überträgt der Bundesrat die Kompetenz zur Regelung der Bearbeitung klassifizierter Bundesratsgeschäfte an die BK.

Absatz 4: Völkerrechtliche Verträge im Bereich der Informationssicherheit, wie mit der EU und der NATO, enthalten 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 kommt vor, dass der Bedarf Informationen innerhalb einer Gruppe rasch zu teilen höher gewichtet wird, als die Wahrung der Vertraulichkeit. 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 zu verursachen. Gemäss bisherigem Recht (vgl. Art. 18 Abs. 3 ISchV) können die Nachrichtendienste und fedpol klassifizierte Informationen vereinfacht handhaben. Denselben Bedarf haben weitere mit Sicherheitsaufgaben betraute Verwaltungseinheiten des Bundes, insbesondere die Gruppe Verteidigung, weshalb die vereinfachte Bearbeitung weiteren Stellen zugänglich gemacht werden soll. Allerdings darf diese Möglichkeit nicht dazu führen, dass für die sicherheitskritischsten Ämter *generell* tiefere Sicherheitsanforderungen gelten als für die anderen Ämter. Deshalb werden die Bedingungen und Modalitäten der vereinfachten Bearbeitung leicht verschärft.

Art. 23 Sicherheitszertifizierung von Informatikmitteln

Die Sicherheitszertifizierung wird im Ausland in der Regel verlangt, wenn klassifizierte Informationen ab der Stufe VERTRAULICH in einem Informatiksystem bearbeitet werden. Im internationalen Verhältnis wird sie immer dann verlangt, wenn geschützte Informationen eines Staates in einem System eines anderen Staates bearbeitet werden sollen. Wird eine solche Zertifizierung auch für ein Informationssystem der Schweiz verlangt, zum Beispiel weil darin klassifizierte Informationen der EU bearbeitet werden sollen, so kann die Fachstelle des Bundes für Informationssicherheit in Zusammenarbeit mit den Krypologen der Armee und den Sicherheitsspezialisten der armasuisse das entsprechende System prüfen und zertifizieren. Massgebend für die Zertifizierung ist der Nachweis der Einhaltung der Mindestanforderungen gemäss Artikel 21 Absatz 1 ISV. Die ISV schliesst eine Lücke, welche die internationale Zusammenarbeit im Sicherheitsbereich bisher erschwert hat. Bisher war für die nationale Zusammenarbeit keine Sicherheitszertifizierung nach Artikel 23 ISV nötig. Informatiksysteme, die auf ein zertifiziertes Informatiksystem zugreifen sollen, müssen unter Umständen ebenfalls zertifiziert werden. Die ISV lässt deshalb die Möglichkeit offen, dass die Zertifizierung auch für die nationale Zusammenarbeit erforderlich sein könnte.

Art. 24 Schutz bei der Gefährdung von klassifizierten Informationen

Entspricht bisherigem 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

Entspricht bisherigem 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. Klassifizierte Informationen des Bundes bleiben Bundesunterlagen im Sinne der Archivierungsgesetzgebung, selbst wenn sie im Rahmen eines Informationsaustausches auch durch Kantone und Dritte bearbeitet werden. Das Vorgehen zur Archivierung auf Bundesebene richtet sich somit auch in diesen Fällen unverändert nach der Archivierungsgesetzgebung.

Absatz 2: Das BAR hat die Aufgabe, den Schutz des 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[19] (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[20] (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 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 bisherige Sicherheitsverfahren gemäss Artikel 14*b*–14*e* CyRV wurde grundsätzlich übernommen.

Absatz 1: Der aktuelle Schutzbedarf ist mittels der 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).

Die bisher 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.

[19] SR **152.11**
[20] SR **152.1**

Absatz 4: Die «nachweisbare» (vgl. Erläuterungen zu Art. 8 Abs. 1 Buchstabe d) 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. Ob eine Änderung der Bedrohungslage wesentlich ist, liegt im Ermessen des Amts.

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.

Absatz 7: Die Fachstelle des Bundes für Informationssicherheit erlässt Mindestvorgaben für die sogenannte Cybersicherheit. Diese Vorgaben gelten übrigens auch für die dezentralen Verwaltungseinheiten sowie für die Organisationen nach Artikel 2 Absatz 4 RVOG, wenn sie auf Informatikmittel der internen Leistungserbringer zugreifen oder ihre eigenen Informatikmittel von diesen betreiben lassen.

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

Neu werden Informatikmittel (vgl. Legaldefinition von 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 bisherigen CyRV, die nur zwei Sicherheitsstufen vorsieht: «Grundschutz» und «erhöhter 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.

Die materiellen Kriterien zur Klassifizierung von Informationen gelten grundsätzlich auch für die Einstufung von Informatikmitteln. Diese sind weitgehend mit den Kriterien, die im Rahmen des Risikomanagements des Bundes für die Beurteilung des Schadenausmasses eines Ereignisses gelten, harmonisiert. Im Gegensatz zu den Einstufungskriterien für klassifizierte Informationen kann im Rahmen der Sicherheitseinstufung der Informatikmittel auch auf finanzielle Kriterien abgestellt werden. 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.

Art. 29 Sicherheitsmassnahmen

Absatz 1: Die bisher vom BACS erlassenen Vorgaben über die Mindestanforderungen für die jeweiligen Sicherheitsstufen nach Artikel 17 ISG für die Bundesverwaltung und die Armee werden neu ab 2025 durch die Fachstelle des Bundes für Informationssicherheit erlassen. Für dezentrale Verwaltungseinheiten, die nicht durch ihr Departement dem ganzen ISG unterstellt werden, und Organisationen nach Artikel 2 Absatz 4 RVOG gelten diese Vorgaben, wenn sie auf Informatikmittel der internen Leistungserbringer der Bundesverwaltung zugreifen oder ihre eigenen von diesen (zum Beispiel durch das Bundesamt für Informatik und Telekommunikation) betreiben lassen. Der «Grundschutz» gilt auch für die Kantone (vgl. Art. 3 ISG), sofern diese unter den Anwendungsbereich des ISG fallen.

Absatz 2: Die Fachstelle 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 Datenschutzberaterinnen und Datenschutzberatern gemäss DSG (vgl. auch Art. 82 Abs. 1 ISG). Die Weisungen 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. Artikel 10 Absatz 2 ISG sowie Erläuterungen zu Artikel 5 Absatz 4 ISV.

Art. 30 Sicherheit beim Betrieb

Absätze 1–3: Die internen Leistungserbringer des Bundes haben bei der Umsetzung der Informationssicherheit eine doppelte Rolle. Einerseits sind sie normale Organisationseinheiten, welche die ISV wie alle anderen Organisationseinheiten 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. Zu diesen Informationen gehören getroffene Schutzmechanismen, welche mehrere Ebenen umfassen, wie Security, Compliance und Backup. Damit können bspw. nicht nur Malware und Ransomware-Angriffe abgewehrt werden. Dies bietet auch Schutz gegen Schäden, die bspw. von Systemausfällen, menschlichem Versagen (bspw. falsche, veraltete Zugriffsberechtigungen usw.) oder auch von „böswilligen“ Benutzern in den eigenen Organisationen verursacht werden. Die 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 4: 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

Hierbei geht es darum festzulegen, wie umfangreich 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». Die entsprechenden Vorgaben gehörten mit bisherigem Recht zum vom BACS erlassenen IT-Grundschutz in der Bundesverwaltung. Eine separate Regelung ist zurzeit nicht notwendig, könnte aber aufgrund der wachsenden Bedeutung dieses «level of assurance» zweckmässig sein.

Art. 32 Personensicherheit

Die Praxis hat gezeigt, dass personenbezogene Sicherheitsrisiken nach bestandener Personensicherheitsprüfung nur in Ausnahmefällen wieder thematisiert werden. Im Sinne einer international üblichen Nachsorge (sogenanntes «aftercare») müssen sicherheitsgeprüfte Mitarbeitende ihrem Arbeitgeber Umstände aus ihrem privaten und beruflichen Umfeld, welche die Sicherheit gefährden, melden. Solche Umstände stellen eine besondere Verwundbarkeit der Mitarbeitenden dar (z.B. Verschuldung im Rahmen einer Spielsucht, aufgedeckte Alkohol- oder Drogensucht durch eine dritte Person, zutage getretene ausserehelicheBeziehung) oder sind Tätigkeiten, die mit erhöhten Risiken verbunden sind (z.B. Reisen in besonders kritische Länder oder intensive Kontakte zu Personen aus solchen Ländern). Für die Mitarbeitenden kann insbesondere die empfundene Verwundbarkeit psychisch besonders belastend sein. Für den Arbeitgeber geht es nicht darum, die Mitarbeitenden auszuspionieren, ständig zu überwachen oder gar zu bestrafen, sondern zusammen mit ihnen in einem vertrauensvollen Verhältnis die allenfalls geeigneten risikomindernden Massnahmen oder Strategien festzulegen. Falls eine heikle Meldung erfolgt, soll das Vorgehen in Zusammenarbeit mit dem Personaldienst oder einer Vertrauensstelle abgestimmt werden.

Zudem müssen die Ämter, Generalsekretariate, Gruppen und die BK 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.

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 BK und 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: Die Vorgaben zur Gewährleistung des physischen Schutzes von Informationen und Informatikmitteln werden heute beim Bund durch mehrere Stellen festgelegt (durch fedpol und das Bundesamt für Bauten und Logistik BBL für die zivile Bundesverwaltung und den Armeestab für die Gruppe V und die Armee). Die bestehenden Vorgaben decken zurzeit den Sicherheitsbedarf hinreichend. Sofern zusätzliche oder bundesweit konsolidierte Vorgaben nötig sein sollten, zum Beispiel in Bezug auf die internationale Harmonisierung der Schutzvorschriften, *kann* die Fachstelle des Bundes für Informationssicherheit nach Konsultation der erwähnten Stellen Mindestanforderungen zum physischen Schutz von Informationen und Informatikmitteln für die Bundesverwaltung und Armee erlassen. Für dezentrale Verwaltungseinheiten und Organisationen nach Artikel 2 Absatz 4 RVOG gelten sie nur, wenn diese klassifizierte Informationen des Bundes bearbeiten, auf Informatikmittel der internen IKT-Leistungserbringer zugreifen oder ihre eigenen von diesen betreiben lassen.

Absätze 1 und 2: Als physische Schutzmassnahmen gelten beispielsweise die Errichtung von Sicherheitszonen (vgl. Art. 35 und ISG-Botschaft, S. 3032 ff.), Eingangskontrollen in Gebäuden, Kameraüberwachungen gewisser Bereiche, Vorrichtungen zur Vernichtung von Informationsträgern oder Arbeitsplatzkontrollen.

Art. 35 Sicherheitszonen

Absätze 1–3: Durch die Schaffung von Sicherheitszonen soll das Schadenpotenzial infolge Spionage oder Sabotage in hochsensiblen Zonen (wie Server- und Führungsräumen oder abhörsichere Räume) reduziert werden (vgl. ISG-Botschaft S. 3015, 3032 ff.). Wenn Personen oder Firmen eine Sicherheitszone nach dieser Verordnung betreten müssen, müssen sie vorgängig einer PSP bzw. einem Betriebssicherheitsverfahren unterstellt werden. Es muss deshalb sichergestellt werden, dass Sicherheitszonen zweckmässig und rechtmässig eingerichtet werden. Deshalb wird vor der Inbetriebnahme eine Kontrolle verlangt, die periodisch wiederholt werden muss. Die Fachstelle des Bundes für Informationssicherheit wird die nötigen Vorgaben erlassen.

Absatz 4: Der Schutz der Informationen und der Informatikmittel in einer Sicherheitszone beginnt bereits ausserhalb der Sicherheitszone. Potenzielle Angreifer verfügen heute über Mittel, mit denen sie elektromagnetische Signale aus der Ferne ausspähen können. Deshalb sollen Verwaltungseinheiten in der unmittelbaren Nähe der Sicherheitszone Sensoren einrichten dürfen, um Ausspähungsversuche zu entdecken und diese abzuwehren. Diese Massnahmen werden in der Regel von den Sicherheitsorganen des Bundes empfohlen. Die Umsetzung liegt allerdings in der Verantwortung der Verwaltungseinheit, welche die Sicherheitszone einrichtet.

7. Abschnitt: Sicherheitsorganisation

Eine wichtige Neuerung in der ISV betrifft die Amtsleitungen. Ihnen werden in der ISV konkrete Aufgaben, Kompetenzen und Verantwortlichkeiten im Bereich der Informationssicherheit übertragen. Die Amtsdirektorin oder der Amtsdirektor darf die Aufgaben einem Mitglied ihrer oder seiner Geschäftsleitung delegieren (Informationssicherheitsverantwortliche). Die Informationssicherheitsverantwortlichen werden das ISMS des Amts beaufsichtigen und alle wichtigen Entscheide im Bereich Informationssicherheit treffen. Die operativen Aufsichtstätigkeiten sind hingegen Aufgabe der Informationssicherheitsbeauftragten. Mit der ISV werden die bisherigen Rollen der «Informatiksicherheitsbeauftragten» und der «Informationsschutzbeauftragten» in der neuen Rolle der «Informationssicherheitsbeauftragten» vereint. Ihre bisherigen 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 den 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 der oder des Informationssicherheitsverantwortlichen, die nur durch eine Person wahrgenommen werden darf.

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

Das rollenbasierte System der ISV ist für die grosse Mehrheit der Verwaltungseinheiten angedacht, bei welchen die Informationssicherheit eine Querschnittsaufgabe darstellt. Bei den IKT-Leistungserbringern des Bundes ist die Gewährleistung der Sicherheit im Betrieb hingegen ein Kernaufgabe. In der Regel verfügen Leistungserbringer auch über eine Sicherheitsabteilung, die von einem Geschäftsleitungsmitglied geführt wird. Da bei diesen Leistungserbringern die Sicherheit bereits hierarchisch organisiert und umgesetzt wird, kann eine Fusion der Rollen «Sicherheitsverantwortliche» und «Sicherheitsbeauftragte» unter Umständen denkbar sein.

Art. 36 Informationssicherheitsverantwortliche der Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe c

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 Informationssicherheitsverantwortung wird auch die persönliche Rechenschaftspflicht delegiert. Aus diesem Grund sollte die Delegation nachweisbar erfolgen (vgl. Erläuterungen Art. 8 Abs. 1 Bst. d).

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 nach Artikel 2 Absatz 1 Buchstabe c

Die Bezeichnung einer offiziellen Stellvertretung ist neu. Diese Rolle entspricht zum guten Teil dem bisherigen Informatiksicherheitsbeauftragten der Verwaltungseinheiten (ISBO).

Die oder der Informationssicherheitsbeauftragte der BK prüft nach Artikel 8 VPSP bei Dritten das Vorliegen einer sicherheitsempfindlichen Tätigkeit, falls dies nicht im Rahmen des Betriebssicherheitsverfahren abgedeckt ist. Bei den Departementen nimmt die Aufgabe jeweils die oder der Informationssicherheitsbeauftragte der Stufe Departement wahr.

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 Informationssicherheitsverantwortung der Departemente

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

Die Departemente können im Übrigen gestützt auf Artikel 47 Absatz 4 RVOG jederzeit Aufgaben und Kompetenzen, welche die ISV den Ämtern, Generalsekretariaten, Gruppen und der BK zuweist, an sich ziehen. So kann ein Departement wie das EDA, das eine zentralisierte Organisationsform hat, seine internen Organisationsbedürfnisse im Rahmen der ISV umsetzen.

Absatz 4: Departementsweite Vorgaben, Massnahmen und Audits werden am besten von den Generalsekretärinnen und Generalsekretären beschlossen. Wenn die Sicherheitsverantwortung in den Ämtern durch die Amtsdirektorinnen oder -direktoren wahrgenommen wird, erwarten diese eine entsprechende hohe Ansiedlung der Person, welche über die Entscheidkompetenz auf Stufe Departement verfügt. Der Fall Xplain in der Bundesverwaltung hat zudem gezeigt, dass eine politisch-strategische Vorfallbegleitung durch die Generalsekretärinnen und Generalsekretäre nötig sein kann. Die Lösung «Generalsekretärin oder Generalsekretär» hat den weiteren Vorteil, dass die departementsübergreifende Koordination in der Generalsekretärenkonferenz stattfinden kann.

Art. 40 Informationssicherheitsbeauftragte der Departemente

Die Bezeichnung einer offiziellen Stellvertretung ist neu (vgl. Art. 81 Abs. 1 ISG). Diese Rolle vereint die Rolle der bisherigen Informatiksicherheitsbeauftragten (ISBD) und Informationsschutzbeauftragten der Departemente. Zusätzlich zu den aufgelisteten Aufgaben und Kompetenzen ist diese Rolle auch für die neue Aufgabe im Bereich der PSP zuständig. Namentlich die Prüfung des Vorliegens einer sicherheitsempfindlichen Tätigkeit bei Dritten nach Artikel 8 VPSP, für die auf das Betriebssicherheitsverfahren verzichtet wird.

Buchstabe f: Weil die Informationssicherheitsbeauftragten nach Artikel 37 und 40 eng zusammenarbeiten müssen, sollte die oder der Informationssicherheitsbeauftragte des Departements nach Artikel 40 bei der Wahl einer neuen Person für die Rolle der oder des Informationssicherheitsbeauftragten der Verwaltungseinheit nach Artikel 37 einbezogen werden. Sie oder er kann insbesondere die Fachkompetenz der zu wählenden Person beurteilen. Die Modalitäten der "Konsultationspflicht" müssen zwischen den Ämtern und dem Departement festgelegt werden.

Buchstabe g: Das Verfahren der Geheimaktenkontrolle wird unverändert übernommen.

Buchstabe h: Bis anhin mussten die jährlichen Berichte der ISBD dem BACS zugestellt werden. Neu haben die Rollenträgerinnen und Rollenträger nach dieser Bestimmung der für die Informationssicherheit verantwortlichen 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 Informationssicherheitsbeauftragte oder -beauftragter des Bundesrates

Neu erhält auch der Bundesrat als verpflichtete Behörde eine oder einen Informationssicherheitsbeauftragten und dessen Stellvertretung gemäss Artikel 81 ISG. Die oder der ernannte Informationssicherheitsbeauftragte übernimmt gemäss Artikel 83 Absatz 3 ISG zugleich die Leitung der Fachstelle des Bundes für Informationssicherheit. Da die Fachstelle Teil des SEPOS im VBS ist, erhält das VBS die Aufgabe, die Informationssicherheitsbeauftragte bzw. den Informationssicherheitsbeauftragten zu bezeichnen.

Art. 42 Fachstelle des Bundes für Informationssicherheit

Absatz 1: Die generellen und weitgehend unterstützenden und koordinierenden 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. 15, weitere Vorgaben in verschiedenen Bereichen nach Art. 17, 21, 23, 27, 29, 31, 34 und 35). Zur Zusammenarbeit zwischen Fachstelle und BACS: vgl. Ziffer 2.3 Buchstabe i.

Buchstabe f: Der Bereich Digitale Transformation und IKT-Lenkung (Bereich DTI) der BK führt die sogenannten Standarddienste (vgl. Art. 4 Abs. 4 der Verordnung vom 25. November

2020[21] über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (VDTI)). Es handelt sich dabei um Leistungen, die in der Bundesverwaltung zentral erbracht und vielfach verwendet werden und gleiche oder ähnliche Bedürfnisse befriedigen. In diesem Zusammenhang verantwortet sie auch Sicherheitsdienste, wie der Einsatz von Threema, die Applikation des Bundes für die sichere Kommunikation auf Smartgeräten. Für Sicherheitslösungen, die von mehreren Departementen und der Armee eingesetzt werden und die im Sinne von Artikel 23 ISV für die Bearbeitung von VERTRAULICH oder GEHEIM klassifizierte Informationen zertifiziert sind, fehlte bis anhin ein bundesweite Bedarfsstelle. Dies hat die Beschaffung, Pflege und Weiterentwicklung von Sicherheitslösungen für die File-Verschlüsselung oder die sichere Videokonferenz erschwert. Die Fachstelle des Bundes soll deshalb die Verantwortung dafür übernehmen. Dadurch wird die Zuständigkeit des Bereichs DTI der BK für die Standarddienste nicht tangiert oder in Frage gestellt.

Absatz 2: 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 3: Die Rolle der nationalen Sicherheitsbehörde, die bisher vom Generalsekretariat des VBS wahrgenommen wurde, wird neu der Fachstelle des Bundes für Informationssicherheit zugeordnet. 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).

Art. 43 Aufgaben und Kompetenzen des BACS

Das Bundesamt für Cybersicherheit (BACS) ist das Kompetenzzentrum des Bundes für Fragen der Cybersicherheit. Sein Kernaufgabe betrifft die Cybersicherheit der Schweiz; dabei ist der Bund grundsätzlich ein «Kunde» von vielen. Das BACS nimmt aber diverse Aufgaben zugunsten der Bundesbehörden wahr, insbesondere in Bezug auf das Vorfallmanagement (vgl. Art. 12 ISV). Es wird zudem die Bundesbehörden beraten und unterstützen und in den Bundesgremien Einsitz nehmen.

Zur Verbesserung der Cybersicherheit des Bundes wird es ermächtigt, in den Netzen der Bundesverwaltung oder im Internet nach technischen Bedrohungen und Schwachstellen zu suchen. Er kann auch Dritte damit beauftragen, zum Beispiel im Rahmen eines Bug-Bounty Programms. Das BACS kann selbstverständlich nicht ohne Erlaubnis die Netzwerke der Armee oder des Nachrichtendiensts durchsuchen.

Das BACS und die Fachstelle des Bundes für Informationssicherheit koordinieren ihre Tätigkeiten, um Doppelspurigkeit zu vermeiden und die Ressourcen möglichst effizient einzusetzen. Beide sind im VBS angesiedelt, was die Zusammenarbeit erleichtert. Vgl. auch Ziffer 2.3 Buchstabe i.

8. Abschnitt: Kosten und Evaluation

Art. 44 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. 45 Evaluation

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

9. Abschnitt: Bearbeitung von Personendaten

Die Artikel 46–48 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 5 Buchstabe c DSG gelten. Die Datenschutzgesetzgebung verlangt dafür eine ausdrückliche Rechtsgrundlage auf Gesetzesebene, die bisher fehlte. Im Rahmen der laufenden Revision des ISG (vgl. Ziff. 2.1) wird die nötige formell-gesetzliche Grundlage geschaffen (vgl. Art. 10*a* ISG).

[21] SR **172.010.58**

Art. 46 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. Die Bearbeitung von Personendaten, die bei der Benutzung der elektronischen Infrastruktur des Bundes anfallen, wird grundsätzlich durch die Artikel 57*i*–57*q* RVOG geregelt. Mit dem neuen Artikel 10*a* ISG wird jedoch die eigene notwendige gesetzliche Grundlage für die Bearbeitung besonders schützenswerter Personendaten geschaffen, welche auch für die nicht elektronische Datenbearbeitung gilt und die Modalitäten des Datenaustauschs verbessert.

Absätze 4 und 5: Bei einem Cyberangriff kommt es regelmässig vor, dass der Angreifer gestohlene Daten im Internet veröffentlicht, wenn das Opfer das Erpressungsgeld nicht bezahlt. Ungeachtet einer potenziellen Strafuntersuchung müssen die Verwaltungseinheiten des Bundes und insbesondere ihre Sicherheitsorgane diese Daten herunterladen und analysieren können, um den Schaden für den Bund beurteilen und die nötigen Schadenbegrenzungsmassnahmen einleiten (z.B. Information der Betroffenen) zu können. Wenn der Cyberangriff bei einer Firma erfolgt, die für den Bund arbeitet, sind meistens nicht nur Informationen des Bundes, sondern auch Daten von anderen Kunden betroffen, für deren Bearbeitung der Bund über keine Rechtsgrundlage verfügt. Diese Bestimmungen ermächtigen die Bundesämter, diese Daten zu bearbeiten. Die Bearbeitung der Daten von Dritten ist nur dann erlaubt, wenn sie für die Beurteilung des Schadens für den Bund nötig sind.

Art. 47 ISMS-Anwendung

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

Art. 48 Elektronische Formulardienste

Absatz 1: Ein Formulardienst ist eine kleine, einfache Anwendung, mit welcher Formulare elektronisch ausgefüllt 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 DSG) 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. 49 Besondere Vollzugsbestimmungen

Sofern das Gesetz dies explizit nicht vorsieht, dürfen nur der Bundesrat oder das zuständige Departement Vorschriften (vgl. Art. 48 Abs. 1 RVOG) erlassen, die für die Kantone verbindlich sind. Da die Fachstelle des Bundes für Informationssicherheit nicht die nötige formell-gesetzliche Kompetenz hat, soll das VBS seine technischen Vorgaben für verbindlich erklären. Dies betrifft insbesondere die Vorgaben nach den Artikeln 21 und 29 ISV.

Art. 50 Aufhebung und Änderung anderer Erlasse

Die CyRV wird aufgehoben. Die ISchV gilt nur noch bis zum 31. Dezember 2023, wodurch ein fliessender Übergang zum neuen Recht besteht (vgl. unten).

Art. 51 Übergangsbestimmungen

Nebst diesen Übergangsbestimmungen 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).

Absätze 1 und 2: Die bestehenden Vorgaben des BACS werden nicht alle bei Inkrafttreten des neuen Gesetzes aufgehoben und ersetzt. Einige wurden kurz vor Inkrafttreten des neuen Rechts angepasst und berücksichtigen dabei viele der neuen Anforderungen (z.B. Vorgaben des Grundschutzes des Bundes). Während der Übergangsfrist sollen je nach Kompetenzbereich gemäss ISV entweder die Fachstelle des Bundes für Informationssicherheit oder das BACS über Ausnahmebewilligungen entscheiden. Beide Organe werden im konkreten Fall entscheiden.

Absätze 3 und 5: Die GSK hat den Klassifizierungskatalog des Bundes erlassen. Dieser wird dann durch die Klassifizierungskataloge nach Artikel 17 ISV ersetzt, die innerhalb einem Jahr nach Inkrafttreten der ISV beschlossen werden müssen (vgl. Art. 51 Abs. 4). Die GSK hat zudem die Weisungen der Koordinationsstelle für den Informationsschutz im Bund über die detaillierten Bearbeitungsvorschriften zum Informationsschutz übernommen. Diese Vorgaben werden innerhalb zwei Jahre vollständig überarbeitet und von der Fachstelle des Bundes für Informationssicherheit verabschiedet.

Absatz 4: Ein ISMS kann man nicht auf der Schnelle aufbauen. Es sind Analyse durchzuführen und Konzepte zu erstellen, die eine gewisse Zeit erfordern. Zudem wird der Bund voraussichtlich ab 2025 über eine ISMS-Anwendung verfügen, um die ISMS-Prozesse zu digitalisieren. Die Frist nach Absatz 4 soll den Ämtern und der BK und den Departementen genügend Zeit geben, um die Arbeiten sorgfältig zu planen und umzusetzen.

Absätze 6 und 7: Ab Inkrafttreten des ISG und der ISV wird im SEPOS die Fachstelle des Bundes für Informationssicherheit schrittweise aufgebaut. Das BACS wird deshalb bis Mitte 2025 seine bisherigen Aufgaben im Bereich Informatiksicherheit weiterhin wahrnehmen und sogar Vorgaben erlassen. Diese Vorgaben haben allerdings eine begrenzte Geltungsdauer, die mit der Frist nach Absatz 3 übereinstimmt.

Art. 52 Inkrafttreten

Die ISV wird mit dem ISG und den restlichen Verordnungen am 1. Januar 2024 in Kraft gesetzt.

Anhang 1

Vgl. Erläuterungen zu Artikel 48.

Anhang 2

Durch die Ablösung der ISchV und der CyRV werden in diversen Verordnungen die Verweise auf das neue Recht aktualisiert und wo nötig der Begriff "Informatiksicherheit" auf "Informationssicherheit" angepasst.

Ziffer 31: Verordnung vom 24. Juni 2009[22] über internationale militärische Kontakte (VIMK): Mit dem ISG und seinen Ausführungsverordnungen müssen die relevanten Organe und Verordnungen aktualisiert werden.

[22] SR **510.215**

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

Vorbemerkungen

Im Rahmen dieser Vorlage erfährt die IAMV nur diejenigen Änderungen, die aufgrund des ISG und des EMBAG notwendig sind. Der identifizierte weitere Anpassungsbedarf der IAMV hingegen ist nicht Teil dieser Vorlage, sondern Gegenstand einer Totalrevision, die die BK bereits an die Hand genommen hat.

Änderungen aufgrund ISG

Bis anhin stützte sich die IAMV hauptsächlich auf das RVOG. Mit den Artikeln 24–26 ISG wird eine formell-gesetzliche Grundlage geschaffen, auf der die IAMV fortan in erster Linie basieren wird. Gestützt auf Artikel 20 Absatz 2 ISG wird es zudem unter bestimmten Voraussetzungen zulässig sein, in IAM-Systemen biometrische Daten neu generell zu verwenden. In der Folge sind in der IAMV die notwendigen Anpassungen vorzunehmen.

Änderungen aufgrund EMBAG

Als Teil des Standarddienstes eIAM hat die Bundesverwaltung einen Authentisierungsdienst für den Zugriff auf ihre Fachanwendungen und E-Government Dienstleistungen (online Verwaltungsleistungen) aufgebaut, der unterdessen eine grosse Verbreitung fand (über 10 Mio. Zugriffe/Monat, über 800 angeschlossene Anwendungen, ca. 2 Mio. Identitäten). Dieser Dienst hat sich bewährt und soll gestützt auf das EMBAG auch den interessierten Kantonen (und ihren Gemeinden) zur Integration mit ihren Anwendungen zur Verfügung gestellt werden. Damit kann für die Bevölkerung ein integrales Login-Verfahren für die Nutzung von digitalen Verwaltungsleistungen über alle drei föderalen Ebenen realisiert und können Synergien für die Verwaltung genutzt werden.
Die entsprechende Leistung wird unter dem Namen AGOV auf den 1. Januar 2024 für die Kantone eingeführt und ermöglicht,

- natürlichen Personen eine elektronische Identität zu generieren und diese für den Zugriff auf alle angeschlossenen Anwendungen für den Bezug von digitalen Verwaltungsleistungen zu verwenden;
- natürlichen Personen ihre bestehenden und von AGOV entsprechend akzeptierten elektronischen Identitäten für den Zugriff auf alle angeschlossenen Anwendungen für den Bezug von digitalen Verwaltungsleistungen zu verwenden;
- Anbietern von digitalen Verwaltungsleistungen ihre Kundinnen und Kunden sicher zu authentisieren und diese Leistung nicht selbst bauen und betreiben zu müssen sowie
- den Verwaltungen der ganzen Schweiz bereit zu sein, die künftige E-ID als Identifikationsmittel für das sichere Authentifizieren einzusetzen und damit zu dessen Verbreitung beizutragen.

An der Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV) werden daher verschiedene Änderungen vorgenommen.

Ingress

Änderungen aufgrund ISG

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. Neu stützt sich die IAMV anstelle des RVOG hauptsächlich auf die genannten Artikel des ISG. Erfasst sind damit auch die IAM-Systeme der Identitätsspeicher. Die Verzeichnisdienste hingegen werden durch das ISG nicht erfasst, weshalb das RVOG diesbezüglich weiterhin aufgeführt werden muss.

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 DSG 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 DSG keine relevante Grösse mehr und brauchen daher nicht mehr erwähnt zu werden. Ein Profiling im Sinne von Artikel 5 Buchstaben f und g DSG findet in IAM-Systemen und Verzeichnisdiensten nicht statt, da diese nicht dazu dienen, persönliche Aspekte von Personen zu *bewerten*.

Änderungen aufgrund EMBAG

Die IAMV behandelt bereits den Verbund von IAM-Systemen, insbesondere den Anschluss externer IAM-Systeme an IAM-Systeme des Bundes (Art. 21 ff.) sowie denjenigen des Bundes an externe IAM-Systeme (Art. 24). Mit dem EMBAG und insbesondere dessen Artikel 11 wurde die gesetzliche Grundlage dafür geschaffen, dass der Bund den Kantonen direkt Leistungen für einen solchen Verbund bereitstellen kann. Der Service AGOV ist Teil des Standarddienstes eIAM und mit der Ausdehnung der Nutzung auf die Kantone und Gemeinden ein typischer Fall der Umsetzung von Artikel 11 EMBAG. Die IAMV regelt betreffend AGOV insbesondere den Vollzug der Absätze 3 bis 5 von Artikel 11 EMBAG. Die vorliegende Revision beinhaltet die für AGOV zusätzlich nötigen Regelungen.

Art. 1 (Gegenstand) wird *nicht* geändert, da sämtliche Stellen, die der IAMV neu zwingend unterstehen sollen (vgl. Ausführungen zu Art. 2 nachfolgend), in der bisherigen Umschreibung «des Bundes» mitenthalten sind. Dies gilt insbesondere auch für die Organisationen nach Artikel 2 Absatz 4 RVOG, die der Bundesverwaltung zuzurechnen sind, da sie mit Verwaltungsaufgaben betraut sind.

Art. 2 Geltungsbereich

Absatz 1

Buchstabe a ergibt sich aus Artikel 2 Absatz 2 Buchstabe b ISG und entspricht dem bisherigen Absatz 1.

Buchstabe b: Der Geltungsbereich für die Armee ist neu und ergibt sich aus Artikel 2 Absatz 2 Buchstabe d ISG.

Absatz 2

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 grundsätzlich auf die Verwaltungseinheiten der dezentralen Bundesverwaltung erweitert wird. Der Bundesrat hat allerdings die Möglichkeit, gestützt auf Artikel 2 Absätze 3 und 4 ISG den Geltungsbereich des ISG einzuschränken. Gleich wie die dezentrale Bundesverwaltung sind neu auch die Organisationen nach Artikel 2 Absatz 4 RVOG für ihre Verwaltungsaufgaben grundsätzlich dem ISG unterstellt (vgl. Art. 2 Abs. 2 Bst. e ISG; der Begriff «Verwaltungsaufgaben» umfasst nur die hoheitlichen Tätigkeiten; damit können allenfalls auch Aufgaben der Bedarfsverwaltung darunterfallen, wenn diese hoheitlich sind [denkbar z. B. im Rahmen eines Beschaffungsverfahrens], was aber die Ausnahme sein dürfte). Auch hier besteht für den Bundesrat jedoch die Möglichkeit, den Geltungsbereich des ISG gestützt auf Artikel 2 Absatz 3 ISG auf die sicherheitsrelevanten Organisationen einzuschränken. Sowohl für die dezentrale Bundesverwaltung als auch für die genannten Organisationen nach RVOG soll der Geltungsbereich der IAMV und der übrigen ISG-Ausführungsverordnungen einheitlich in der ISV festgelegt werden, weshalb in der IAMV lediglich ein entsprechender Verweis vorgesehen wird.

Die Inhalte des bisherigen 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 möglich, sofern keine entgegenstehenden Bestimmungen des Bundesrechts bestehen).

Art. 5 IAM-Systeme

Absatz 1: Neben den bereits bisher in der IAM aufgeführten verantwortlichen Organen der zentralen Bundesverwaltung werden die weiteren verantwortlichen Bundesorgane der zentralen Bundesverwaltung (Bst. a Ziff. 2, d und f) von IAM-Systemen aufgeführt.

Bst. a Ziff. 1: Da der Bereich DTI der BK innerhalb der Bundesverwaltung für den Standarddienst eIAM zuständig ist, ist er es zur Gewährleistung einer kohärenten Steuerung auch für den Teil AGOV dieses Dienstes.

Bst. c: Hier wird anstelle der Führungsunterstützungsbasis (FUB) die Gruppe Verteidigung genannt, da die Verantwortung neu generell bei dieser sein soll; wie die Verantwortung alsdann V-intern konkret geregelt wird, soll nicht Regelungsgegenstand der IAMV sein.

Absatz 2: Aktuell erfolgt keine Kontrolle der Bearbeitung der Personendaten in IAM-Systemen. Gestützt auf Artikel 26 Buchstabe e ISG, der eine periodische Kontrolle der Bearbeitung von Personendaten durch eine externe Stelle vorsieht, wird betreffend die IAMS-Systeme der zentralen Bundesverwaltung ein entsprechender zusätzlicher Absatz eingefügt.

Absatz 3: Mit Rücksicht auf die – mehr oder weniger ausgeprägten – Organisationsautonomien der Armee, der Verwaltungseinheiten der dezentralen Bundesverwaltung sowie der Organisationen nach Artikel 2 Absatz 4 RVOG soll auf Verordnungsstufe lediglich festgelegt werden, dass die genannten Stellen jeweils für ihre eigenen IAM-Systeme verantwortlich sind. Aus demselben Grund wird bei diesen Stellen darauf verzichtet, eine periodische Kontrolle der Bearbeitung von Personendaten durch eine externe Stelle zwingend vorzusehen.

Hinsichtlich IAM-Systeme der Armee ist zudem festzuhalten, dass diese die einsatzrelevanten Systeme der Armee versorgen, wogegen die IAM-Systeme nach Artikel 5 Absatz 1 Buchstabe c die Systeme der Militärverwaltung versorgt. Die fraglichen IAM-Systeme sind aufgrund unterschiedlicher rechtlicher Normen zur Datenbearbeitung und Verantwortlichkeit zu differenzieren und separat der IAMV zu unterstellen.

Absatz 4: 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 sinngemäss 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 5: Aufgrund der neuen Absätze 2–4 wird der bisherige Absatz 2 inhaltlich unverändert zu Absatz 5.

Art. 6 Bst. b Ziff. 3

Neu ist auch hier (vgl. Erläuterung zu Art. 5 Abs. 1 Bst. c oben) die Gruppe Verteidigung anstelle der FUB zu nennen.

Art. 7 Bst. b

Die AGOV für die Inanspruchnahme von E-Government-Leistungen nutzenden Personen müssen eine klare Ansprechstelle für die Ausübung ihres Berichtigungs- und Vernichtungsrecht haben. Dies ist wie für das Auskunftsrecht das für den Dienst verantwortliche Organ nach Artikel 5.

Art. 9 Bst. b

Im Rahmen von AGOV werden im eIAM System nicht bloss Personendaten von Nutzenden von (E-Government-)Systemen des Bundes, sondern neu auch solche von Nutzenden von Informationssystemen von Kantonen und Gemeinden geführt. Häufig wird es sich um die gleichen Personen handeln, die einmal eine Anwendung des Bundes und ein anderes Mal eine solche eines Kantons oder einer Gemeinde zur Inanspruchnahme derer digitalen Verwaltungsleistungen nutzen. Sinn und Zweck von AGOV ist, dass die Nutzenden nicht für jede Nutzung ein separates Login mit separater Identifizierung eröffnen und bedienen müssen.

Art. 11 Abs. 2 und 3

Die bisherigen 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 Datenschutzgesetzes zu überarbeiten.

Absatz 2: An die Stelle des Verbots der Bearbeitung von Persönlichkeitsprofilen tritt ein Verbot des Profiling sowie Profiling mit hohem Risiko (vgl. Art. 5 Bst. f und g DSG). Darunter fällt grundsätzlich jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Werden aber beispiels-

weise Randdaten und damit das Benutzerverhalten zwecks Erkennung von Unregelmässigkeiten und potentiellen Cyber-Angriffen (Fraud Detection) ausgewertet, so sind diese Datenbearbeitungsvorgänge nicht vom Profiling-Begriff des DSG erfasst, da im Zentrum nicht das Zusammentragen und die Analyse verschiedenster persönlicher Aspekte einer bestimmten Person stehen, sondern die Wahrung der Informationssicherheit.

Da der bisherige Absatz 2 per 1. September 2023 durch die neue Datenschutzverordnung vom 31. August 2022 aufgehoben worden ist, wird vom 1. September 2023 bis zum 31. Dezember 2023 (die vorliegende Änderung soll per 1. Januar 2024 in Kraft treten) bezüglich Verbots des Bearbeitens von Persönlichkeitsprofilen bzw. des Profilings und Profilings mit hohem Risiko eine Lücke bestehen, die jedoch aufgrund der kurzen Dauer vertretbar sein sollte.

Absatz 3: Neu gelten biometrische Daten, die eine Person eindeutig identifizieren, 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. 13) neu grundsätzlich in allen IAM-Systemen bearbeitet werden, in denen es zur risikogerechten Identifizierung erforderlich ist. Vgl. dazu auch die nachfolgende Erläuterung zum Anhang Buchstabe a.

Art. 12 Abs. 4

Damit der IAM-Dienst des Bundes im Rahmen von AGOV die Vermittlungsfunktion von anerkannten Identitäten auch der Kantone wahrnehmen kann (ID-Broker), kann er Daten automatisiert aus den IAM-Systemen der entsprechenden zuliefernden Kantone übernehmen. Die Prozesse, Schnittstellen und Sicherheitsmassnahmen sind Gegenstand der Weisungen gemäss Artikel 24 Absatz 2 und der Vereinbarungen gemäss Artikel 24 Absatz 1 Buchstabe b.

Art. 13 Abs. 4 Bst. a

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[23] 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. Dies gilt auch für bundesexterne Anbieter von Verzeichnisdiensten, insbesondere wenn diese Anbieter nicht bereits ein IAM-System betreiben. Der Verordnungstext wird daher entsprechend ergänzt.

Zudem wird im letzten Teilsatz von Absatz 2 die Umschreibung «vordefinierten» gestrichen, so dass nur noch von «Minimalanforderungen» die Rede ist (der gestrichene Begriff bringt keinen Mehrwert). Inhaltlich bleibt die Bestimmung unverändert.

Art. 20 IAM-Gesamtsystem

Gemäss bisherigem 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 übrigen IAM-Systemen des Bundes (z. B. der eidgenössischen Gerichte) verbunden werden können, weshalb neu von IAM-Systemen *des Bundes* gesprochen wird.

Wie bis anhin und in der Praxis gelebt soll eine Verbindung von externen IAM-Systemen mit den IAM-Systemen des Bundes (einzelnes System oder Gesamtsystem) möglich sein (vgl. aktuellen Art. 21, der vorsieht, dass externe IAM-Systeme unter gewissen Voraussetzungen an die IAM-Systeme des Bundes angeschlossen werden können). Neu soll dies bereits in Artikel 20 vorgesehen werden.

[23] SR **510.91**

Art. 21 Einleitungssatz und Bst. a

Allgemein: Artikel 21 regelt die Bedingungen unter denen (bundes)externe IAM-Systeme an die IAM-Systeme des Bundes angeschlossen werden können. Dieser Anschluss wird immer vollständig sein, was aber keineswegs die Aufgabe aller Datensouveränität bedeutet. Nach Artikel 9 Buchstabe a zum Beispiel dürfen lediglich Personendaten verarbeitet werden, die Ressourcen der Bundesverwaltung verwenden; dies ist eine zusätzliche Rahmenbedingung auch für Artikel 21. So schliesst sich zum Beispiel ein Kanton zwar an IAM Bund an, steuert aber nur die Personendaten bei, die für die Nutzung der Bundesressource benötigt werden, keinesfalls pauschal alle. Zudem ist hierbei keine passive Bereitstellung, sondern eine proaktive Sendung durch das kantonale IAM-System vorgesehen. Der Kanton hat also immer die Kontrolle darüber, welche Daten über welche Personen preisgegeben werden.

Einleitungssatz: Wenn ein externes IAM-System nach Artikel 21 mit den IAM-Systemen des Bundes verbunden werden soll, so ist es insbesondere aus Sicherheitsgründen zwingend, dass sich die fraglichen Betreiberinnen und Betreiber, mit Ausnahme der Kantone, der IAMV unterwerfen. Für den Anschluss von IAM-Systemen von Kantonen an jene des Bundes ist es wichtig, dass in den kantonalen IAM-Systemen eine mindestens gleichwertige Informationssicherheit gewährleistet ist. Es müssen aber nicht gleichzeitig alle (übrigen) Vorgaben der IAMV für die Kantone auch gelten. Dies ist auch vor dem Hintergrund der verfassungsrechtlichen Zuständigkeitsordnung zwischen Bund und Kantonen zielführend. Der Einleitungssatz wird entsprechend dem Gesagten ergänzt.

Buchstabe a entspricht der bisherigen Fassung, jedoch ergänzt um IAM-Systeme des Fürstentums Liechtenstein. Damit wird einem Ersuchen des Fürstentums nachgekommen.

Art. 24 Abs. 1 Bst. a

Damit AGOV seinen Nutzen entfalten kann, muss das IAM-System des Bundes mit denjenigen der interessierten Kantone und Gemeinden verbunden werden. Dieser Fall wird neu in Artikel 24 aufgenommen. Aus systematischen Gründen wird dazu Absatz 1 Buchstabe a mit diesem Fall ergänzt. Für den Anschluss wird eine Vereinbarung nach Absatz 1 Buchstabe b abgeschlossen, die die Beziehung in rechtlicher, organisatorischer und technischer Hinsicht regelt. Zur organisatorischen Regelung gehört auch die finanzielle im Sinne von Artikel 11 Absatz 4 EMBAG. Angeschlossen werden darf nur, wenn die angeschlossenen Systeme über die nötigen Rechtsgrundlagen verfügen, etwa weil die Rechte und Pflichten Privater in Bezug auf den Datenschutz oder das Verfahrensrecht betroffen sind (Art. 11 Abs. 5 EMBAG).

Anhang

Änderungen aufgrund ISG

Buchstabe a: 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 (bisher war 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 (Ziff. 13) integriert (Bst. g kann somit aufgehoben werden). Sie 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. Weiter dürfen biometrische Daten aufgrund mangelnder formell-rechtlicher Grundlage nicht zwischen den Systemen verschiedener Verantwortlicher bekanntgegeben werden. Schliesslich sind die biometrischen Daten nach dem Wegfall der Zugangsberechtigung zu vernichten (vgl. Art. 20 Abs. 3 ISG und Art. 14 Abs. 2 IAMV).

Die bisherige Ziffer 11 (Gesichtsbild für Ausweise) ist neu in einer separaten Ziffer zu führen (Ziff. 14), da das nicht biometrische Gesichtsbild bzw. die einfache Fotografie in sämtlichen IAM-Systemen (und folglich in allen drei Spalten) geführt werden soll. Neu ist nur von «Gesichtsbild» die Rede, da nicht nur Bilder auf Ausweisen gemeint sind, sondern z.B. auch die Bilder in Skype.

Buchstabe c: Neu wird eine Führung der Büronummer auch in den IAM-Systemen mit Personen nach Artikel 8 und 9 Buchstabe b vorgesehen, weil die Supportprozesse des digitalen Arbeitsplatzes diese Information benötigen.

Buchstabe e: In Ziffer 7 wird präzisiert, dass die Passwörter kryptographisch gesichert sein müssen, dies per hinreichend vertraulicher Verschlüsselung oder ausreichend verlässlichem *«hashing*

with salting». Dies sollte eigentlich selbstverständlich sein (alle internen Bewirtschaftungsregeln für Passwörter enthalten die Vorgabe, Passworte ausschliesslich verschlüsselt oder gesalzen/gehasht zu speichern). Dennoch kommt es in der Praxis ab und an vor, dass Passwörter schlecht gesichert sind und «geknackt» werden können.

Buchstabe f: Hier werden dem Wortlaut des ISG entsprechend (Einleitungssatz und Ziff. 2) zwei sprachliche Anpassungen vorgenommen.

Buchstabe g wird aufgehoben (vgl. Erläuterung oben).

Änderungen aufgrund EMBAG

Bst. a Ziff. 4 und 5, Bst. c Ziff. 2 und Bst. e Ziff. 11

Zu den in AGOV zu führenden Personendaten gehören auch die Nationalität und der Geburtsort, die private Postadresse sowie die Authentisierungsqualität. Diese Daten werden den konsumierenden Informationssystemen im Rahmen der Authentisierungsleistung weitergegeben. Die entsprechenden Fachanwendungen benutzen sie zur Geschäftsbearbeitung (bspw. Bewilligungsverfahren, Steuerveranlagung, Finanzhilfen, Dienstleistungen, etc.). Nationalität und Geburtsort werden auch in der künftigen E-ID geführt werden (vgl. Art. 2 Abs. 2 Bst. e und f Vorentwurf zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise [E-ID-Gesetz, BGEID] vom 29. Juni 2022). Die Authentisierungsqualität zu kennen ist bei E-Government Anwendungen zur weiteren Bearbeitung durch die Fachanwendung notwendig. Je nach Fachanwendung bzw. nach Leistungsgegenstand können die Anforderungen an die Qualität der Abklärung der Identität unterschiedlich sein.

Die konsumierenden Systeme müssen zur Bearbeitung der Daten über die nötigen (datenschutzrechtlichen) Grundlagen verfügen (Art. 11 Abs. 5 EMBAG). Im Falle der Kantone haben diese die nötigen Grundlagen im kantonalen Recht zu schaffen.

3.3 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

Mit der VPSP soll eine bundesrätliche 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.

In der Systematik des ISG ist der Bundesrat grundsätzlich eine von mehreren verpflichteten Behörden nach Artikel 2 Absatz 1 ISG, die alle gleichgesetzt sind. Als verpflichtete Behörde ist er nach Artikel 84 Absatz 1 ISG für den Erlass der für seinen Zuständigkeitsbereich erforderlichen Ausführungsbestimmungen zuständig. Um eine Harmonisierung der Sicherheitsniveaus zwischen den verpflichteten Behörden zu erzielen, hat der Gesetzgeber in Artikel 84 Absatz 3 ISG festgehalten, dass die Ausführungsbestimmungen, die der Bundesrat für seinen eigenen Zuständigkeitsbereich erlässt, auch für die anderen verpflichteten Behörden sinngemäss gelten, sofern diese keine eigenen Vorschriften erlassen. Es gibt allerdings Bereiche, für welche das ISG den anderen verpflichteten Behörden diese «Opt-Out»-Kompetenz entzieht. So macht es keinen Sinn, dass sowohl der Bundesrat als auch beispielsweise das Parlament, die Bundesgerichte oder die Nationalbank je ein Prüfverfahren für die Personensicherheitsprüfungen festlegen oder die Organisation der Fachstellen die PSP regeln. Hierzu darf es nur eine einzige Regelung geben und der Gesetzgeber hat die entsprechende Rechtsetzungskompetenz ausdrücklich dem Bundesrat übertragen. Wenn der Bundesrat als «verpflichtete Behörde» Ausführungsbestimmungen erlässt (vgl. z.B. Art. 26 und 28 ISG), können die anderen verpflichteten Behörden eigene Ausführungsbestimmungen erlassen. Wenn das Gesetz eine Vollzugskompetenz ausdrücklich dem Bundesrat (vgl. z.B. Art. 48, 73, 80 oder 83 abs. 3 ISG) überträgt, ist dieser alleine zuständig. In diesen Fällen gibt es keine eigene Regelungskompetenz für die anderen Bundesbehörden.

Der Gesetzgeber hat in Artikel 48 ISG ausdrücklich *einzig* dem Bundesrat die Kompetenz erteilt, Vollzugsbestimmungen zu den Regelungsgegenständen der Absätzen 1 und 2 übertragen. Hingegen hat der Bundesrat als verpflichtete Behörde nach Artikel 2 Absatz 1 ISG spezifische Vollzugsaufgaben für seinen eigenen Bereich, das heisst die Bundesverwaltung und die Armee. Vgl. auch Erläuterungen zu Artikel 2.

Art. 2 Geltungsbereich

Die VPSP gilt grundsätzlich für alle Behörden und Organisationen, die dem ISG unterstehen. Für die dezentralen Verwaltungseinheiten und Organisationen mit Verwaltungsaufgaben nach Artikel 2 Absatz 4 RVOG ist der Geltungsbereich eingeschränkt: Nur diejenigen, die unter den Geltungsbereich der ISV fallen, fallen unter den Geltungsbereich der VPSP bezüglich PSP nach ISG. Dezentrale Verwaltungseinheiten, die vom Geltungsbereich des BPG erfasst werden, können ebenfalls von der Vertrauenswürdigkeitsprüfungen nach Artikel 20*b* BPG betroffen sein und in diesem Zusammenhang unter den Geltungsbereich der VPSP fallen.

Die VPSP gilt auch für die vom Bundesrat unabhängigen verpflichteten Bundesbehörden nach Artikel 2 Absatz 1 ISG. Der Gesetzgeber hat nämlich in Artikel 48 ISG dem Bundesrat die alleinige Kompetenz erteilt, die Modalitäten des Prüfverfahrens und die Organisation der Fachstellen PSP zu regeln. Hingegen bleiben die verpflichteten Behörden für den Erlass ihrer Funktionenlisten oder für die Bezeichnung der einleitenden und entscheidenden Stellen zuständig (vgl. Erläuterungen zu Artikel 1).

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[24] und 6*a* Absatz 2 des Ausweisgesetzes[25] vom 22. Juni 2001 können auch für bestimmte Personen im Bereich der Ausstellung von Ausweisen Sicherheitsprüfungen im Sinne von Artikel 6 der bisherigen PSPV durchgeführt werden. In der VPSP sollen bewusst keine Funktionenlisten dafür geführt werden. Bei zwingendem Bedarf einer PSP wäre diese über ein Betriebssicherheitsverfahren bei den entsprechenden Unternehmen abgedeckt.

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 Bundesrats fallen (beispielsweise die Bundesanwaltschaft), müssen ihre Funktionenlisten selber erlassen.

Absatz 4: Dieser Absatz entspricht mehrheitlich der geltenden Regelung von Artikel 1 Absatz 3 PSPVK. Bereits in der Projektphase werden durch Projektanten VERTRAULICH oder GEHEIM klassifizierte Informationen bearbeitet. Dadurch ist bereits zu diesem Zeitpunkt der Bedarf einer Zuverlässigkeitskontrolle gegeben. Mit der Aufnahme der Projektanten einer neuen Kernanlage und Inhaber einer Rahmenbewilligung ist somit der gesamte Zyklus, in dem VERTRAULICH oder GEHEIM klassifizierte Informationen bearbeitet werden müssen, abgedeckt.

Art. 4 Änderung

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 bisher. Das VBS soll deshalb die Funktionenlisten zentral bewirtschaften und sie auf Antrag der Departemente und der BK laufend aktualisieren. Dabei soll es die Fachstelle des Bundes für Informationssicherheit beiziehen. Die nationale Netzgesellschaft stellt Änderungsanträge der Funktionenliste nach StromVG erst nach Absprache mit der Elektrizitätskommission an das Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation.

Art. 5 Veröffentlichung, Aufbewahrung und Bekanntgabe

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. Zur Sicherheitsempfindlichkeit der Funktionenlisten, vgl. Ziffer 2.5 Buchstabe e.

Art. 6 Aktualitätsprüfung

Absatz 1: Die Prüfung der Richtigkeit der Funktionenlisten erfordert einen erheblichen Aufwand. Es besteht aber ein klarer Bedarf 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 alle drei Jahre 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 erfolgt. 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. Der Antrag wird durch die Bundes-

[24] SR **142.20**
[25] SR **143.1**

kanzlei oder die Departemente gestellt. Diese sollen vorgängig ihre Informationssicherheitsbeauftragte oder ihren Informationssicherheitsbeauftragten konsultieren. 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 Kantonsangestellten, 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 von Dritten, die für eine verpflichtete Behörde oder Organisation einen Auftrag ausführen, der die Durchführung einer sicherheitsempfindlichen Tätigkeit beinhaltet, können nicht im Voraus festgelegt werden, sondern ergeben sich aus den Notwendigkeiten der einzelnen Aufträge. Damit auch hier die Notwendigkeit der Prüfung gewährleistet ist, sollen die Entscheide zentralisiert erfolgen. Beim Entscheid geht es um die Prüfung der Rechtmässigkeit der Durchführung der Prüfung und die Fragestellung: Liegt im konkreten Fall tatsächlich eine sicherheitsempfindliche Tätigkeit vor?

Art. 9 Ausserordentliche Zuverlässigkeitskontrolle des Eidgenössischen Nuklearsicherheitsinspektorats

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

4. Abschnitt: Zuordnung zu den 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[26] (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. Entscheidend ist, ob die Bearbeitung klassifizierter Informationen für die Aufgabenerfüllung im Rahmen der Funktion erforderlich ist. Zum Kriterium der Regelmässigkeit für die Durchführung von PSP vgl. ISG-Botschaft, Ziffer 1.2.5, S. 2985, sowie Erläuterungen zu Art. 29 ISG, S. 3036-3037.

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 beinhalten oder bei deren Ausübung Personen in der Lage sind, beispielsweise durch Sabotage, die öffentlichen Interessen nach Artikel 1 Absatz 2 ISG erheblich zu beeinträchtigen. Ob die Anwender von Informatikmitteln eine sicherheitsempfindliche Tätigkeit ausüben, entscheidet sich allein aufgrund der Klassifizierung der zu bearbeitenden 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 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 Ausweisung 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 Sicherheitszonen 1 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.

[26] SR **142.31**

Absatz 2 Buchstaben a–c: Vgl. Erläuterung zu Absatz 1 Buchstaben a–c.

Absatz 2 Buchstaben d und e: Personen, die für den Nachrichtendienst des Bundes (NDB) oder seine Aufsichtsbehörde, den militärischen Nachrichtendienst und für den Dienst Cyber und elektromagnetische Aktionen (CEA) sicherheitsempfindliche Tätigkeiten ausüben, tun dies regelmässig in höchst sensitiven Bereichen. Ihre Tätigkeiten sollen daher der Prüfstufe erweiterte Personensicherheitsprüfung zugeordnet sein.

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

Art. 11 Prüfung der Vertrauenswürdigkeit nach dem BPG

Absatz 1 Buchstabe a: Bei den hoheitlichen Tätigkeiten des im Ausland eingesetzten Personals und des der Versetzungspflicht unterstellten Personals des EDA (vgl. Art. 3 Bst. a und b der Verordnung des EDA vom 20. September 2002[27] 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: Potenzielle finanzielle Schäden von 50–500 Millionen Franken werden im vorliegenden Kontext als erheblich erachtet.

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

Absatz 2 Buchstaben a und b: 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[28] (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 für 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 c: Unter Leiterin und Leiter der dezentralen Verwaltungseinheiten sind die Geschäftsführerinnen und Geschäftsführer gemeint. Diese sollen ebenfalls aufgrund der hohen Reputationsschaden bei Verfehlungen dieser Funktionsträgerinnen und Funktionsträger einer erweiterten PSP unterstehen (vgl. Artikel 11 Abs. 2 Bst. a und b). Jedoch fallen nur diejenigen unter diesen Buchstaben, welche dem BPG unterstellt sind. Beispielsweise nicht unter das BPG fallen die Leitung der ausserparlamentarischen Kommissionen oder die Geschäftsführung der FINMA. Bei den restlichen dezentralen Verwaltungseinheiten sind die Prüfgründe nach ISG massgebend.

Absatz 2 Buchstabe d: Im vorliegenden Kontext entspricht ein potentieller finanzieller Schaden von mehr als 500 Millionen Franken der Auswirkung «hoch» und von mehr als einer Milliarde Franken als «sehr hoch».

Absatz 2 Buchstabe e: Eine vorschriftswidrige oder unsachgemässe Leistung des Personals von fedpol im Bereich der Bekämpfung der Schwerstkriminalität in Bundeskompetenz, wie beispielsweise die Bekämpfung von Terrorismus, gewalttätigem Extremismus und organisierter sowie übriger transnationaler Kriminalität, kann öffentlichen Interessen des Bundes erheblich gefährden.

Absatz 2 Buchstabe f: Tätigkeiten der Angestellten der Fachstellen PSP nach Artikel 16 Absatz 1, welche als sicherheitspolizeiliche Tätigkeiten gelten, sollen ebenfalls der erweiterten Personensicherheitsprüfung unterzogen werden.

Art. 12 Prüfungen nach dem Militärgesetz vom 3. Februar 1995[29] (MG)

Absatz 1 Buchstabe a: Nicht jede Tätigkeit im Ausland von Angehörigen der Armee in Uniform 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.

[27] SR **172.220.111.343.3**
[28] SR **172.220.111.3**
[29] SR **510.10**

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: Bis anhin konnte 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.

Absätze 3 und 4: Dieser Absatz entspricht inhaltlich weitgehend der geltenden Regelung nach Artikel 5 Absätze 2 und 3 PSPV.

Art. 13 Zuverlässigkeitskontrollen nach dem Kernenergiegesetz vom 21. März 2003[30] (KEG)

Dieser Artikel entspricht inhaltlich im Wesentlichen der geltenden Regelung nach Artikel 3 PSPVK mit der Ergänzung der Projektanten einer neuen Kernanlage sowie der Inhaber einer Rahmenbewilligung. Absatz 1 Buchstabe b ersetzt verschiedene Kategorien von Personen, für die nach der bisherigen PSPVK eine PSP erforderlich war, durch die Nennung von sicherheitsrelevanten Tätigkeiten als Prüfgrund, in Analogie zu anderen tätigkeitsorientierten Bestimmungen in der VPSP. Die Formulierung «erheblich beeinträchtigen» nimmt Tätigkeiten aus, deren Schadenpotential bei ungetreuer Ausübung eine PSP nicht rechtfertigt. Absatz 1 Buchstabe b folgt den Grundsätzen der nuklearen Sicherheit und der Nutzung der Kernenergie, wonach im Sinne der Vorsorge alle Vorkehren zu treffen sind, die nach der Erfahrung und dem Stand von Wissenschaft und Technik notwendig sind und, soweit sie angemessen sind, zu einer weiteren Verminderung der Gefährdung beitragen (Art. 4 Abs. 3 KEG). Die Bestimmung entspricht hinsichtlich des Personenkreises der Praxis.

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.

Einer Personensicherheitsprüfung zu unterziehen sind bspw. Personen, welche eigenständigen Zugang zu elektrischen Anlagen haben, da diese Personen in der Lage sind, innert kurzer Zeit Einfluss auf die Versorgungssicherheit zu nehmen.

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 bewusst 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 zu 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: Bei einem Betriebssicherheitsverfahren ist die Fachstelle Betriebssicherheit die einleitende und entscheidende Stelle. Wird aber gemäss Artikel 53 Absatz 2 ISG auf das Verfahren verzichtet und nur die PSP durchgeführt, so leitet die Auftraggeberin die PSP ein, nachdem die oder der Informationssicherheitsbeauftragte des Departements geprüft hat, ob wirklich eine sicherheitsempfindliche Tätigkeit durch die angestellten Dritten ausgeführt wird. Die Auftraggeberin ist zudem auch die entscheidende Stelle und in der Praxis üblicherweise die Beschaffungsstelle.

[30] SR **732.1**

Absatz 4: Dieser Absatz entspricht den bisherigen Artikeln 2 Absatz 2 und 4 Absatz 1 PSPVK mit Ergänzung der Projektanten einer neuen Kernanlage sowie der Inhaber einer Rahmenbewilligung (vgl. Erläuterungen zu Art. 4 Abs. 4).

Absatz 6: Damit die Fachstellen PSP ihre Arbeit effizient erledigen können, müssen sie wissen, wer bei den einzelnen Behörden für die Einleitung von Prüfungen und für den Entscheid über die Ausübung der Funktion zuständig ist.

Absatz 7: Aufgrund der Tatsache, dass immer noch Prüfungen mit physischen Formularen eingeleitet werden, soll die einleitende Stelle solche Originaldokumente aufbewahren. Sie bewahrt diese solange auf, wie die betroffene Person die sicherheitsempfindliche Tätigkeit ausübt, längstens jedoch zehn Jahre.

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 3 Buchstabe d die Funktionen des SEPOS im VBS mit Führungsaufgaben gegenüber der Fachstelle PSP VBS überprüfen. Damit sind die Staatssekretärin beziehungsweise der Staatssekretär, 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 dem Buchstaben d.

Im Übrigen gelten die Vorschriften über den Ausstand gemäss Artikel 10 Verwaltungsverfahrensgesetz vom 20. Dezember 1968[31].

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 6 Absatz 6 DSG genügt.

Die Fachstellen überprüfen zudem, ob die notwendigen Angaben für die Prüfung vorhanden sind. Dies sind insbesondere die notwendigen Daten zur Identifikation der Person, die bisherigen Wohnsitze sowie elektronische Kontaktdaten wie beispielsweise die E-Mailadresse.

Art. 18 Mitwirkung

Die ganze Sicherheitsprüfung wäre unwirksam, 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: Bisher erfolgten die Datenbankabfragen hauptsächlich durch die Fachstelle PSP VBS. Mit dem Inkrafttreten des ISG und der VPSP werden die beiden Fachstellen die Daten der ihnen zugewiesenen Fälle selbst erheben. 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

[31] SR **172.021**

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 Fachstellen PSP entscheiden frei, ob die Befragung bei einer ordentlichen Wiederholung der Prüfung nach Artikel 26 notwendig ist, wenn sich die Risikolage kaum geändert hat. In der Praxis wird dies eher eine Ausnahme sein.

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. Erfüllt eine Person mehrere Prüfgründe, sollen die Prüfungen aus verfahrensökonomischen Gründen zusammengefasst werden. Ist eine Person aufgrund dieser Voraussetzungen durch beide Fachstellen PSP zu prüfen, soll nur die Fachstelle PSP BK die Prüfung durchführen. Der Grund für die Wahl der 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 den 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. Diese risikomindernden Massnahmen personalrechtlicher Natur stützen sich auf Artikel 39 Absatz 1 Buchstabe b bzw. Artikel 41 Absatz 3 ISG (vergl. auch Botschaft Artikel 42) und werden in Artikel 22 Buchstabe b VPSP spezifiziert. Der Arbeitgeber kann gestützt auf Artikel 24 Absatz 2 BPG solche Massnahmen anordnen. Die Grundlage, besonders schützenswerte Personendaten zu bearbeiten, ergibt sich für den Bund aus Artikel 27 Absatz 2 BPG, soweit dies für die Wahrung von wichtigen Interessen erforderlich ist.

Art. 23 Mitteilung

Absatz 1: Unterstehen Personen aufgrund verschiedener Prüfgründe mehreren Prüfungen, die nicht gleichzeitig erfolgen, sollen risikorelevante Feststellungen 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 der Prüfungen ein Risiko in Bezug auf die Armeewaffe festgestellt, so dürfen die Fachstellen PSP der zuständigen militärischen Behörde dies 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 Mittelung des Entscheids über die Ausübung der Tätigkeit

Die entscheidende Stelle trägt die Verantwortung für die geprüfte Person und entscheidet deshalb über die Ausübung der Tätigkeit. Allfällige von den Fachstellen PSP empfohlene 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.

Die zeitnahe Mitteilung des Entscheids über die Ausübung der Tätigkeit ist unter anderem für den Zutritt zu militärischen Anlagen oder zu Sicherheitszonen nötig. Sie ist auch für die Ausstellung einer Sicherheitsbescheinigung 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. Für Angehörige der Armee entspricht die Beurteilung des Gefährdungs- oder Missbrauchspotenzials nach Artikel 113 Absatz 4 Buchstabe d MG einer Grundsicherheitsprüfung nach ISG.

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. Ein Beispiel hierfür sind die Beurteilungen des Gefährdungs- oder Missbrauchspotenzials nach Artikel 113 Absatz 4 Buchstabe b MG, welche nur ausserordentlich wiederholt werden, beispielsweise in Verdachtsfällen nach Artikel 12 Absatz 3 Buchstabe c VPSP.

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, soll die entscheidende Stelle allenfalls mit angemessenen Massnahmen nach Artikel 21. Absatz 2 ISG dafür sorgen, dass sich diese Risiken bis zum Abschluss der Prüfung nicht verwirklichen können. Dies kann insbesondere durch den vorläufigen Entzug gewisser Tätigkeiten oder vorläufige 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

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. Bisher wurde eine «clearance» nur im internationalen Verhältnis verlangt. Vermehrt erwarten auch inländische Stellen, dass Personen, die an klassifizierten Projekten oder Sitzungen teilnehmen sollen, eine Sicherheitsbescheinigung vorlegen. Eine «clearance» kann für beide Zwecke beantragt und ausgestellt werden.

7. Abschnitt: Bearbeitung von Personendaten

Art. 31 Verantwortung für den Datenschutz und die Datensicherheit

In Anwendung von Artikel 33 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. Solche unabhängigen Stellen sind beispielsweise die interne Revision, externe Auditoren sowie die Datenschutzberaterin bzw. der Datenschutzberater oder der EDÖB.

8. Abschnitt: Vollzugsbestimmungen

Art. 33 Elektronischer Geschäftsverkehr

Für Bundesangestellte ist neu der elektronische Geschäftsverkehr mit den Fachstellen PSP Pflicht. Nach der aktuellen Praxis ist eine Verpflichtung der Allgemeinbevölkerung zur elektronischen Kommunikation jedoch nicht zumutbar (vgl. Botschaft zum Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben; BBl 2022 804). Personen, die nicht beim Bund angestellt sind, können deshalb verlangen, dass der Geschäftsverkehr mit ihnen in Papierform erfolgt. Die Korrespondenz zwischen Behörden, erfolgt weiterhin elektronisch. In Bezug auf den elektronischen Rechtsverkehr mit den Gerichten stellt Art. 48 ISG i. V. m. Art. 35 VPSP eine spezialgesetzliche Bestimmung gemäss Art. 1 Abs. 2 Ausführungsreglement des Bundesverwaltungsgerichts über den elektronischen Rechtsverkehr mit Parteien[32] dar.

[32] SR **173.320.6**

Art. 34 Gebührenerhebung

Die Kosten für die Prüfungen aus der zentralen Bundesverwaltung und der Armee sollen zentral beim VBS budgetiert werden. Dazu gehören auch die vom ISG und BPG auferlegten Prüfungen für sämtliche verpflichtete Behörden und Organisationen. 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 Fachstelle erfordern, können die Leistungen nur erbracht werden, wenn der Fachstelle diese zusätzlichen Mittel auch tatsächlich gewährt werden. Eine bundesinterne Kompensation dieser Mittel ist ausgeschlossen.

9. Abschnitt: Schlussbestimmungen

Art. 36 Aufhebung und Änderung 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 bisherigen Departementsverordnungen werden daher aufgehoben. Ebenso aufgehoben wird die geltende Verordnung über die Personensicherheitsprüfungen, die mit der vorliegenden Verordnung totalrevidiert wird. Ferner wird die Verordnung über die Personensicherheitsprüfungen im Bereich Kernanlagen aufgehoben, da deren Inhalte, soweit noch erforderlich, in die vorliegende Verordnung integriert werden. Aufgrund des Umfangs der Änderung anderer Erlasse erfolgt die entsprechende Regelung im Anhang 8. Die Erläuterung dazu folgt weiter unten.

Art. 37 Übergangsbestimmungen

Wenn bei Inkrafttreten der Verordnung Prüfungen noch hängig sind, müssen die Fachstellen PSP in Zusammenarbeit mit den einleitenden Stellen prüfen, ob die Prüfung noch durchgeführt werden muss und gegebenenfalls in welcher Prüfstufe. Prüfungen, die nicht mehr durchgeführt werden, werden nach Massgabe von Artikel 17 Absatz 3 eingestellt. Die bisherige erweiterte PSP mit Befragung wird neu in die erweiterte PSP eingestuft. Im SIBAD werden diese Prüfungen gekennzeichnet sein, damit weiterhin ersichtlich ist, dass eine Befragung stattgefunden hat.

Die Erklärungen zu den bisherigen 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. 38 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 Kapitel 2.5 Bst. e und zu Art. 5).

Anhang 7 Datenerhebung

Es liegt in der Natur der PSP, dass höchstpersönliche Daten über die Lebensführung der zu prüfenden Person, insbesondere über ihre engen persönlichen Beziehungen und familiären Verhältnisse, ihre finanzielle Lage und ihre Beziehungen zum Ausland, erhoben und bearbeitet werden (vgl. Art. 27 Abs. 2 ISG). Ohne diese Daten kann keine fachgerechte Beurteilung des Sicherheitsrisikos vorgenommen werden. Das ISG selbst legt die nötigen Schranken für die Bearbeitung dieser Daten fest, die nur dann erhoben und bearbeitet werden, wenn sie sicherheitsrelevant sind (vgl. z.B. Art. 27 Abs. 2 und 3 sowie Art. 34 ISG). Daten über die Ausübung verfassungsmässiger Rechte dürfen beispielsweise nur dann bearbeitet werden, wenn ein konkreter Verdacht besteht, dass die zu prüfende Person diese Rechte ausübt, um Tätigkeiten vorzubereiten oder auszuüben, welche die öffentlichen Interessen nach Artikel 1 Absatz 2 ISG gefährden (z.B. die Entscheidungs- und Handlungsfähigkeit der Behörden und Organisationen des Bundes oder die innere und äussere Sicherheit der Schweiz). Die Daten werden zudem risikogerecht erhoben und bearbeitet. 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. Werden Daten erhoben, die für die Beurteilung des Sicherheitsrisikos nicht relevant sind, so ist der Aufwand für die Fachstellen PSP unnötig höher. Deshalb sorgen sowohl das Recht als auch die Fachstellen PSP selbst dafür, dass sie nur die nötigen Daten erheben und bearbeiten.

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 Aufhebung und Änderung anderer Erlasse

1. VVMH

Damit die Fachstellen via Abrufverfahren die Daten aus Hoogan beziehen können, ist eine Grundlage vorausgesetzt.

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. 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 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. Verordnung über das Nationale Ermittlungssystem

Mit dem ISG erhalten die Fachstellen eine neue gesetzliche Grundlage, welche in der Verordnung über das Nationale Ermittlungssystem angepasst werden muss.

4. VIMK

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

5. Verordnung vom 16. Dezember 2009[33] über militärische und andere Informationssysteme im VBS (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.

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

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

7. 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.

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

3.4 Verordnung über das Betriebssicherheitsverfahren (VBSV)

Einleitende Bemerkungen

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

- 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, insbesondere 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).
- Die Regelungen des Betriebssicherheitsverfahrens finden parallel zu den Regelungen des öffentlichen Beschaffungswesens Anwendung. Die Erarbeitung der VBSV ist in enger Zusammenarbeit mit den zentralen Beschaffungsstellen (Bundesamt für Bauten und Logistik, armasuisse) erfolgt, so dass sichergestellt werden kann, dass Betriebssicherheits- und Beschaffungsverfahren optimal aufeinander abgestimmt sind.

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 ISG 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.

Absätze 2 und 3: 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. 2.6 Bst. b). Zur Geltung für die verpflichteten Behörden vgl. Erläuterungen zu Artikel 1 VPSP. Die in Absatz 2 erwähnte Deckungsgleichheit muss sich auch auf die dezentrale Bundesverwaltung beziehen. Der Geltungsbereich der VBSV richtet sich nach demjenigen der diesbezüglich einschlägigen ISV.

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 «Betriebs» 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 Betriebs 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: Bereits das ISG benennt in Artikel 51 Absatz 2 die Fachstelle Betriebssicherheitsverfahren (Fachstelle BS) als für die Durchführung des Verfahrens zuständig. Die Verordnungsbestimmung weist nur noch darauf hin, dass diese im VBS angesiedelt sein wird.

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 Präjudizien für das Vergabeverfahren geschaffen. Durch das neue Betriebssicherheitsverfahren wird die Risikomanagementmethode zur Reduktion nachrichtendienstlicher Ausspähung vollständig abgelöst.

Art. 4 Antrag auf Einleitung des Verfahrens

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

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 möglichst genaue Beschreibung der Bauleistung, Lieferung oder Dienstleistung dient der Fachstelle BS insbesondere dann als Identifizierungsmerkmal, 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.

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. Dies sind 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 überprüft werden.
- 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 Betriebs, 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 Meldung geeigneter Betriebe

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 Betriebs 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: 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. Gemäss Artikel 56 Absatz 1 Buchstabe a ISG kann die Fachstelle BS zur Beurteilung der Eignung der Betriebe bei diesen selber entsprechende Daten erheben. 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.

Falsche Angaben stellen im Gegensatz zu verweigerten Angaben zwar kein Hindernis 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 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.

Art. 10 Ausschluss vom Verfahren

Absatz 1: Sowohl Artikel 44 des Bundesgesetzes vom 21. Juni 2019[37]über das öffentliche Beschaffungswesen (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.

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

4. Abschnitt: Sicherheitskonzept

Art. 12 Inhalt und Prüfung des Sicherheitskonzepts

Absatz 1: 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 (Schlüsselhandling, Raumüberwachung), personelle (Ausbildung, Personensicherheitsprüfungen), technische (Einsatz von Informatikmitteln) und physische Massnahmen (Einbruchsicherungen). Falls im Rahmen der Eignungsprüfung nach Artikel 55–58 ISG gewisse Risiken festgestellt werden, die mit organisatorischen Massnahmen hinreichend herabgesetzt werden können, so werden diese ins Sicherheitskonzept integriert.

Absatz 2: 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 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. 13 Betriebssicherheitsbeauftragte

Absatz 1: Ein Betrieb, welcher von der Auftraggeberin zur Eignungsprüfung angemeldet wird, soll eine Betriebssicherheitsbeauftragte oder einen Betriebssicherheitsbeauftragten 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 Betriebs 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.

Absatz 2 Buchstabe a: Für eine effiziente und effektive Einflussnahme auf die Informationssicherheit des Betriebs 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. 14 Mitteilung des Zuschlags

Absatz 1: Rahmenverträge dürften in der Regel ein auslösendes 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 Buchstabe b 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. 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 Möglichkeit der 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 abschliessenden Aufzählungen konkretisieren Artikel 63 Absatz 2 ISG hinsichtlich des Inhalts der Meldepflicht betreffend sicherheitsrelevante Änderungen im Betrieb.

Absatz 3: 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 4: 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 Betriebs 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

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

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.

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 VBS hat bezüglich Auswahl der Revisionsstelle ein gewisses Ermessen.

7. Abschnitt: Leistungen der Fachstelle BS zugunsten der Kantone

Art. 24

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. Eine vollständige Überprüfung und laufende Kontrolle von Firmen, die kantonale Aufträge erhalten, macht aus Sicht des Bundes wenig Sinn. Der Bund hat keinen Bedarf, solchen Firmen eine BSE zu erteilen. Hingegen kann eine Überprüfung der Vertrauenswürdigkeit von Firmen in Zusammenarbeit mit dem NDB durchaus sinnvoll sein. Die Möglichkeit soll den Kantonen offenstehen, sofern sie eine genügende formell-gesetzliche Grundlage dafür haben und eine Leistungsvereinbarung mit dem VBS abgeschlossen haben, in der die Modalitäten und die Finanzierung des Leistungsbezugs festgelegt werden.

8. Abschnitt: Schlussbestimmungen

Art. 25 Aufhebung und Änderung anderer Erlasse

Vergleiche die Erläuterungen zu Anhang 2 unten.

Art. 26 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. 27 Inkrafttreten

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

Anhang 1

Im Anhang finden sich nun die Daten des Informationssystems zum Betriebssicherheitsverfahren, welche gemäss Artikel 25 Absatz 5 VBSV aus der MIV entfernt werden.

Anhang 2

I: Aufhebung anderer Erlasse

Das nur im VBS anwendbare Geheimschutzverfahren war in der bisherigen Geheimschutzverordnung geregelt. Das neu bundesweit anwendbare Betriebssicherheitsverfahren deckt materiell die Regelungsmaterie der Geheimschutzverordnung ab, weshalb diese ersatzlos aufgehoben wurde.

II: Änderung anderer Erlasse

1. Nachrichtendienstverordnung vom 16. August 2017[40] (NDV)

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 NDV, wo die Fachstelle BS noch nicht aufgeführt war. Dies wird mit der vorliegenden Ziffer 10.6 nachgeholt.

2. VIMK

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

3. MIV

Die Aufführung der in der MIV genannten Daten erfolgt neu im Anhang der VBSV, weshalb die entsprechenden Streichungen vorgenommen werden können.

[40] SR **121.1**